2006

Classifying quadratic number fields up to Arf equivalence

Jeonghun Kim
Louisiana State University and Agricultural and Mechanical College

CLASSIFYING QUADRATIC NUMBER FIELDS UP TO ARF EQUIVALENCE

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Jeonghun Kim
B.S., Chonbuk National University, 1997
M.S., Louisiana State University, 2001
August 2006

Acknowledgments

It is a pleasure to express my sincere appreciation to Dr. Robert Perlis. Without his invaluable help and guidance, this dissertation would not be completed.

I also thank my committee for their service: Dr. Jurgen Hurrelbrink, Dr. Richard A. Litherland, Dr. Gestur Olafsson, Dr. Bogdan Oporowski and Dr. Jerry Trahan.

I am grateful to professors for my undergraduate studies. In particular, I thank Dr. Yonghwan Cho. He encouraged me to study abroad.

Most of all, I would like to thank my wife, Soyoung, for her support and patience.

Finally I want to thank my parents and my family for their constant love and encouragement.

Table of Contents

Abstract

Two number fields K and L are said to be Arf equivalent if there exists a bijection $T : \Omega_K \longrightarrow \Omega_L$ of places of K and of L such that K_P and L_{TP} are locally Arf equivalent for every place $P \in \Omega_K$. That is, $|K_P^*/K_P^{*2}| = |L_{TP}^*/L_{TP}^{*2}|$, $\text{type}[(\ ,\ )_P] = \text{type}[(\ ,\ )_{TP}]$, and $\text{Arf}(r_P) = \text{Arf}(r_{TP})$ for every place $P \in \Omega_K$, where r_P is the local Artin root number function and $(\ ,\ )_P$ is the Hilbert symbol on K_P^*. In this dissertation, an infinite set of quadratic number fields are classified up to Arf equivalence.

Introduction

Throughout this introduction V is an n-dimensional vector space over $\mathbb{F}_2$. Let B be a bilinear form on V. In general there are exactly two types of bilinear forms B. B is of type II if $B(a,a) = 0$ for all $a \in V$ and is of type I otherwise. A type II bilinear form always has a symplectic basis meaning a basis in which the matrix of B is an orthogonal sum of matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Clearly a type II space (V,B) can occur only when V is an even dimensional vector space. A classical refinement r of the inner product space (V,B) is an $\mathbb{F}_2$ counterpart of a quadratic form. By definition a classical refinement is a function $r : V \longrightarrow \mathbb{F}_2$ that satisfies the following:

$$r(a+b) = B(a,b) + r(a) + r(b) \quad \text{for } a,b \in V.$$

There are 2^n classical refinements of a non-degenerate type II inner product space (V,B). The problem is that there are no classical refinements for type I spaces since $B(a,a) = r(0) = 0$ for every $a \in V$. In recent years it was realized that there is a new kind of "multiplicative" refinement r (called *refinement*) that exists for any B. A refinement is a map $r : V \longrightarrow \mathbb{C}^*$ on (V,B) satisfying

$$r(a+b) = \beta(a,b) \cdot r(a) \cdot r(b) \quad \text{for } a,b \in V$$

where $\beta(a,b) = (-1)^{B(a,b)} \in \mathbb{C}$ is the "multiplicative lift" of B from $\mathbb{F}_2$ to $\mathbb{C}$. The new concept was introduced by topologists. In this new setting every non-degenerate bilinear space allows exactly 2^n refinements.

Let $f(x)$ be a polynomial in $\mathbb{Q}[x]$. Then $\mathbb{Q}(\alpha)$ is said to be a *number field*, where α is a root of $f(x)$ in $\overline{\mathbb{Q}}$. Suppose a valuation is given for K. The valuation defines a metric topology. Two valuations are called equivalent if their topologies are the same. An equivalence class of valuations is called a *place* of K. Suppose P is a place

of a number field K. Then there is the completion K_P of K. In K_P every Cauchy sequence of K_P with respect to the valuation $|\ |_P$ has a limit in K_P. The local square classes K_P^*/K_P^{*2} is a finite dimensional vector space over $\mathbb{F}_2$. For the local square classes K_P^*/K_P^{*2} there is a well-known multiplicative bilinear form $(\ ,\ )_P$ which is called the *Hilbert symbol* defined by

$$(a,b)_P = \begin{cases} 1 & \text{if } ax^2+by^2=1 \text{ has a solution } (x,y) \text{ in } K_P \times K_P \\ -1 & \text{otherwise ,} \end{cases} \tag{1}$$

for $a, b \in K_P^*/K_P^{*2}$. Our goal is to find a refinement of the Hilbert symbol. Suppose $\rho : \mathrm{Gal}\,(\overline{K}|K) \longrightarrow \mathbf{GL}_n(\mathbb{C})$ is a representation. Then there is a corresponding complex number $W(\rho)$ which is called a *global root number*. It comes from the functional equation of the Artin L-function $L(s,\rho)$. Fröhlich-Queyrut showed that $W(\rho) = 1$ if ρ is a real representation. Deligne showed that $W(\rho)$ can be expressed as a product

$$W(\rho) = \prod_{P \in \Omega_K} W_P(\rho),$$

where $W_P(\rho)$ is called a *local root number* and Ω_K is the set of all places of K. We consider the following specific representation. Let $a \in K$. We define a real representation $\rho_a : \mathrm{Gal}\,(\overline{K}|K) \longrightarrow \mathbf{GL}_1(\mathbb{C})$ by $\rho_a(g) = \frac{g(\sqrt{a})}{\sqrt{a}}$. By Deligne, $1 = \prod_P W_P(\rho_a)$. To simplify notation we write $r_P(a)$ in place of $W_P(\rho_a)$. So $r_P : K_P^*/K_P^{*2} \longrightarrow \mathbb{C}^*$. Tate showed that the local root number function satisfies $r_P(ab) = (a,b)_P \cdot r_P(a) \cdot r_P(b)$. Now we have two number fields K and L with places P of K and Q of L. Then we can find local square classes and local root number functions r_P and r_Q. Two number fields K and L are Arf equivalent if and only if there exists a bijection T of places of K and L such that $|K_P^*/K_P^{*2}| = |L_{TP}^*/L_{TP}^{*2}|$, type$[(\ ,\ )_P]$=type$[(\ ,\ )_{TP}]$ and Arf(r_P)=Arf(r_{TP}). Perlis showed that Arf equivalence implies Witt equivalence. Czogała and Carpenter classified quadratic number

fields up to Witt equivalence. There are exactly seven Witt equivalence classes of quadratic number fields. So there are at least seven Arf equivalence classes in quadratic number fields. The natural question is "how many Arf equivalence classes exist in quadratic number fields?". Is it finite or infinite? In fact, there are infinitely many Arf equivalence classes of quadratic number fields. On the other hand there are exactly ten equivalence classes of the form $\mathbb{Q}(\sqrt{ep})$, where $e = \pm 1$ and p is a rational positive prime. They are represented by $\mathbb{Q}(\sqrt{\pm 2})$, $\mathbb{Q}(\sqrt{\pm 3})$, $\mathbb{Q}(\sqrt{\pm 5})$, $\mathbb{Q}(\sqrt{\pm 7})$, $\mathbb{Q}(\sqrt{\pm 17})$. This result will be proved in Chapter 3.

1. Preliminaries

1.1 Valuations and Local Fields

Throughout F will denote a field and F^* will denote the multiplicative group of all non-zero elements of F.

Definition 1.1. A valuation of a field F is a function $|\ |$ from F into the nonnegative real numbers such that

$$|a| = 0 \Longleftrightarrow a = 0, \tag{1.2}$$

$$|\,ab| = |\,a||\,b|, \tag{1.3}$$

$$|\,a + b| \leqslant |\,a| + |\,b|. \tag{1.4}$$

The last condition is called the *triangle inequality*. We start with the field $\mathbb{Q}$ of rational numbers. It is clear that the ordinary absolute value function on $\mathbb{Q}$ is a valuation; from now on it is expressed by $|\ |_\infty$. The trivial valuation, denoted by $|\ |_0$, is defined by $|\,0| = 0$ and $|\,r| = 1$ if $r \in \mathbb{Q}^*$. Now we want to find other valuations on $\mathbb{Q}$. Let p be a fixed prime number and let c be a positive real number which is less than 1. Any non-zero rational number r can be written uniquely as

$$r = p^\alpha \frac{a}{b}$$

where $a,\ b \in \mathbb{Z},\ p \nmid a,\ p \nmid b$ and $\alpha \in \mathbb{Z}$. We define

$$|\,r|_p = c^\alpha,\ \textit{and} \quad |\,0|_p = 0.$$

Then $|\ |_p$ is a valuation which is called a p-adic valuation. Usually we choose $\frac{1}{p}$ for c; then we speak of the normalized p-adic valuation on $\mathbb{Q}$. Every p-adic valuation has the following property.

$$|\,x + y|_p \leq \max(|\,x|_p\,, |\,y|_p),$$

for all $x,\ y \in \mathbb{Q}$.

This property is called the *strong triangle inequality*. If a valuation satisfies the strong triangle inequality, it is called a non-archimedean valuation. So any p-adic valuation is a non-archimedean valuation. On the other hand, if a valuation does not satisfy the strong triangle inequality, it is called an archimedean valuation. The valuation $|\ |_\infty$ is an archimedean valuation. For a given field F with a valuation $|\ |$ we can define a metric space (F, d) by defining a metric d as follows:

$$d(x, y) = |\, x - y| \ \text{ for all } x, y \in F.$$

Metric spaces are always Hausdorff. If two valuations define the same topologies, we shall say that they are equivalent.

Lemma 1.2. *Let $|\ |_1$ and $|\ |_2$ valuations on the same field F. Then the following statements are equivalent:*

(1) The two valuations are equivalent,

(2) $|\, \alpha|_1 < 1 \Longleftrightarrow |\, \alpha|_2 < 1$,

(3) There is a positive number ν such that $|\, \alpha|_1{}^\nu = |\, \alpha|_2$ for all $\alpha \in F$.

Proof. see 11:4, p. 5 in [15]. □

If p and q are different primes, then $|\ |_p$ is not equivalent to $|\ |_q$ as valuations on $\mathbb{Q}$ since $|\, p\,|_p^\nu < 1$ for any $\nu > 0$ but $|\, p\,|_q = 1$.

Theorem 1.3. *(Ostrowski) Every non-trivial valuation on $\mathbb{Q}$ is equivalent to $|\ |_p$ for some prime integer p or to $|\ |_\infty$.*

Proof. See Theorem 2.1, p. 16 in [4]. □

We call an equivalence class of a non-trivial valuation a *place*.

Definition 1.4. The field F is called complete with respect to the valuation $|\ |$ if every Cauchy sequence of F with respect to $|\ |$ has a limit in F.

Let $\{a_n\}$ and $\{b_n\}$ be Cauchy sequences of F with respect to a valuation $|\ |$. We define addition and multiplication by

$$\{a_n\} + \{b_n\} = \{a_n + b_n\} \quad \text{and} \quad \{a_n\}\{b_n\} = \{a_n b_n\}.$$

Then the set A of all Cauchy sequences of F is a commutative ring with unity. Also the set M of all null sequences in A is an ideal of A. The ideal generated by M and a non-null sequence in A is the whole ring A. Thus M is a maximal ideal in A. So A/M is a field called the completion of F with respect to the valuation $|\ |$ and is denoted by $\hat{F}$. The map $f : F \to \hat{F}$ defined by $f(a) = \{a\} + M$ is an embedding. Thus $\hat{F}$ contains an isomorphic copy of F. We can define a valuation on $\hat{F}$ by $|\{a_n\} + M| = \lim_{n\to\infty} |a_n|$. Then the valuation on $\hat{F}$ is an extension of $|\ |$ and is well-defined since $\{|a_n|\}$ is a Cauchy sequence in $\mathbb{R}$ and $\mathbb{R}$ is complete.

Theorem 1.5. *Let F be a field with a valuation $|\ |$. Then there exists a field $\hat{F}$ which is called completion of F with respect to $|\ |$ such that $\hat{F}$ is a complete field with respect to a valuation extending $|\ |$ and F is dense in $\hat{F}$.*

Proof. See 11:13, p. 10 in [15]. □

Definition 1.6. The completion of the field $\mathbb{Q}$ of rational numbers with respect to a p-adic valuation $|\ |_p$ is called the field of p-adic numbers which is denoted by $\mathbb{Q}_p$.

Remark 1.7. The completion of $\mathbb{Q}$ with respect to the valuation $|\ |_\infty$ is $\mathbb{R}$.

Any p-adic number α can be expressed as

$$\alpha = \sum_{j=n}^{\infty} \alpha_j p^j,$$

where $n \in \mathbb{Z}$ and $a_j \in \{0, 1, \cdots, p-1\}$. If $n_0 = \min\{j : a_j \neq 0\}$, then $|\alpha|_p = |p|_p^{n_o}$ (see Theorem 2.1, p. 35 in [2]). Let $\mathbb{Z}_p = \{\sum_{j=0}^{\infty} \alpha_j p^j\}$. Then $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$ called *the ring of p-adic integers*. The subset $p\mathbb{Z}_p = \{\sum_{j=1}^{\infty} \alpha_j p^j\}$ is the unique prime ideal in $\mathbb{Z}_p$ and $\mathbb{Z}_p$ is a local ring (the set of all non-units forms an ideal). This implies that $\mathbb{Z}_p^* = \{\sum_{j=0}^{\infty} a_j p^j \mid a_0 \in \mathbb{F}_p^*\}$. The residue class field $\mathbb{Z}_p/p\mathbb{Z}_p$ is a finite field with p elements. So $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Theorem 1.8. *(Hensel's Lemma) Suppose $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$. Then the following are equivalent:*

(1) $f(x)$ has a root in $\mathbb{Z}_p$.

(2) There is an integer a_n such that $f(a_n) = 0 \pmod{p^n}$ for each $n \geq 0$.

Proof. See p. 45 in [18]. □

Corollary 1.9. *The number -1 is a square in $\mathbb{Q}_p$ if and only if $p \equiv 1 \pmod 4$.*

1.2 Quadratic Forms and Witt Rings

Throughout this section a field F is a field of characteristic different from 2.

Definition 1.10. Let V be a finite dimensional vector space over a field F. A symmetric bilinear form B on V is a function

$$B : V \times V \longrightarrow F$$

with the following properties:

$$B(x, y+z) = B(x, y) + B(x, z), \text{ for all } x, y, z \in V \tag{1.5}$$

$$B(\alpha x, y) = \alpha B(x, y), \text{ for all } x, y \in V \text{ and all } \alpha \in F \tag{1.6}$$

$$B(x, y) = B(y, x), \text{ for all } x, y \in V \tag{1.7}$$

B is non-degenerate if, given $x \neq 0$, there is y with $B(x, y) \neq 0$. The pair (V, B) consisting of a vector space V and a non-degenerate bilinear form B on V is called

an *inner product space*. For a given symmetric bilinear form B on V the map $Q : V \longrightarrow F$ defined by $Q(x) = B(x, x)$ is called a quadratic map. A quadratic map Q has the following properties:

$$Q(\alpha x) = \alpha^2 Q(x), \tag{1.8}$$

$$Q(x + y) = Q(x) + Q(y) + 2B(x, y), \tag{1.9}$$

$$Q(\sum_i \alpha_i x_i) = \sum_i \alpha_i^2 Q(x_i) + 2\sum_{i<j} \alpha_i \alpha_j B(x_i, x_j). \tag{1.10}$$

In fact, Q and B determine each other by the relation

$$Q(x + y) - Q(x) - Q(y) = 2B(x, y).$$

(recall that we are assuming $\mathrm{char}(F) \neq 2$ in this section.) The pair (V, Q) is called a quadratic space.

Definition 1.11. Two inner product spaces (V, B), (V', B') are said to be *isometric* if there exists an F-linear isomorphism $T : V \longrightarrow V'$ such that

$$B'(T(x), T(y)) = B(x, y) \text{ for all } x, y \in V$$

For a given inner product space (V, B), let $x_1, x_2, \cdots, x_n$ be a basis of V. Then we can associate an $n \times n$ matrix $A = (a_{ij})$ to (V, B) where $a_{ij} = B(x_i, x_j)$. We write $A = M_{B,\{x_1,\cdots,x_n\}}$. By the definition of B, the matrix A is symmetric. Suppose $y_1, y_2, \cdots, y_n$ is another basis of V. Then the corresponding matrix $A' = (B(y_i, y_j))$ is given by

$$A' = P^t A P$$

where P is a nonsingular $n \times n$ matrix (p_{ij}) and $y_i = p_{i1}x_1 + \cdots + p_{in}x_n$ for $i = 1, \cdots, n$.

Definition 1.12. Two $n \times n$ matrices A and B are *congruent* if there exists a nonsingular matrix P such that $A = P^t B P$.

Congruence is an equivalence relation. Moreover there is a one-to-one correspondence between isometry classes of n dimensional quadratic spaces and congruence classes of $n \times n$ symmetric matrices with entries in F.

Definition 1.13. An n-ary quadratic form f over a field F is a homogeneous polynomial of degree 2 in n variables, i.e.,

$$f(x_1, x_2, \cdots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \in F[x_1, x_2, \cdots, x_n] =: F[x].$$

We usually express f by $f(x) = \sum_{i,j} a'_{ij} x_i x_j$, where $a'_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$. Then for a given n-ary quadratic form a symmetric $n \times n$ matrix (a'_{ij}) is determined and is denoted by M_f. Say two n-ary quadratic forms f and g are equivalent, denoted $f \simeq g$, if $M_f = P^t M_g P$ for some nonsingular matrix P. There is a one-to-one correspondence between the equivalence classes of n-ary quadratic forms and the isometry classes of n dimensional inner product spaces.

Proposition 1.14. *Let B be a symmetric bilinear form on V, and let A be the matrix of B in some basis of V. Then the following statements are equivalent:*
(1) A is a nonsingular matrix.
(2) The map $\phi : V \longrightarrow \mathrm{Hom}_F(V, F)$ defined by $\phi(x) = B(\_, x)$ is an isomorphism.
(3) For $x \in V$, $B(x, y) = 0$ for all $y \in V$ implies that $x = 0$.

Definition 1.15. Let S be a subspace of V. Then we define *the orthogonal complement* of S by

$$S^{\perp} = \{x \in V \mid B(x, s) = 0 \text{ for all } s \in S\}.$$

In particular $V^{\perp}$ is so-called the *radical* of (V, B). By Proposition 1.14,

$$(V, B) \text{ is regular } \iff V^{\perp} = \{0\}$$

Definition 1.16. Let $(V_1, B_1), (V_2, B_2)$ be inner product spaces. We define an inner product space (V, B), where $V = V_1 \bigoplus V_2$ and $B : V \times V \longrightarrow F$ is the map defined by

$$B((x_1, x_2), (y_1, y_2)) = B_1(x_1, y_1) + B_2(x_2, y_2).$$

Then B is symmetric bilinear and non-degenerate, and $B(V_1, V_2) = 0$. The pair (V, B) is called the orthogonal sum of (V_1, B_1) and (V_2, B_2) and is denoted $V_1 \perp V_2$. A quadratic space (V, f) is non-degenerate if the associated bilinear space (V, B) is non-degenerate. We let $\langle d \rangle$ denote the isometry class of the 1-dimensional inner product space corresponding to the bilinear form dx^2. It is clear that

$$\langle d \rangle \text{ is regular } \iff d \in F^*.$$

For the next theorem, recall that F denote a field of characteristic $\neq 2$.

Theorem 1.17. *(Diagonalization) Let (V, B) be an inner product space over F, then there exists $d_1, \cdots, d_n$ in F such that $V \simeq \langle d_1 \rangle \perp \cdots \perp \langle d_n \rangle$. In other words, any n-ary quadratic form is equivalent to a diagonal form $d_1 x_1^2 + \cdots + d_n x_n^2$.*

Proof. See Corollary 2.4, p. 10 in [11]. □

From now on we express $\langle d_1 \rangle \perp \cdots \perp \langle d_n \rangle$ by $\langle d_1, \cdots, d_n \rangle$. Also $n\langle d \rangle$ will be used for n-ary form $\langle d, \cdots, d \rangle$. The above Theorem says that every quadratic form over F can be diagonalized, *i.e.*, it can be expressed as an orthogonal sum of 1-dimensional quadratic forms. Let f be an n-ary quadratic form. We say that f is *isotropic* if there exists a nonzero vector $v \in F^n$ such that $f(v) = 0$. If f is not isotropic, it is called *anisotropic*. A form that is isometric to an anisotropic form is itself anisotropic. On the other hand, if $f(v) = 0$ for all $v \in F^n$, then we shall say that f is totally isotropic. Any 2-dimensional quadratic form that is isometric to the quadratic form $\langle 1, -1 \rangle$ is called *the hyperbolic plane* and is denoted by $\mathbb{H}$.

The hyperbolic plane is both regular and isotropic. Any 2-dimensional quadratic form which is both regular and isotropic is isometric to $\mathbb{H}$ (See Theorem 3.2, p. 12 in [11]). An orthogonal sum of hyperbolic planes is called a hyperbolic space.

Lemma 1.18. *(Witt Decomposition) Let q be a regular quadratic form. Then*

$$q \simeq m\langle 1, -1\rangle \perp q_a \text{ for some } m \in \mathbb{N} \cup \{0\},$$

where q_a is an anisotropic form on F.

Proof. See Theorem 4.1, p. 15 in [11]. □

Lemma 1.19. *(Witt Cancellation) If q, q_1, q_2 are arbitrary quadratic forms, then*

$$q \perp q_1 \simeq q \perp q_2 \Longrightarrow q_1 \simeq q_2.$$

Proof. See Theorem 4.2, p. 15 in [11]. □

It is clear that if two regular quadratic forms are isometric, then their anisotropic parts are also isometric by Lemma 1.18 and Lemma 1.19. We say two quadratic forms q_1 and q_2, possibly of different dimensions, are Witt equivalent(denoted by $q_1 \sim q_2$) if their anisotropic parts are isometric. We shall denote by $W(F)$ the Witt equivalence classes of regular quadratic forms. Now we want to give a ring structure to $W(F)$. We already introduced an operation $\perp$. We define another operation $\otimes$ by

$$q \otimes q' = \langle a_1 b_1, a_1 b_2, \cdots, a_n b_m\rangle,$$

where $q = \langle a_1, \cdots, a_n\rangle$ and $q' = \langle b_1, \cdots, b_m\rangle$.

Remark 1.20. The operations $\perp$ and $\otimes$ on $W(F)$ are well-defined. Also the following are satisfied:

(1) $q_1 \perp (q_2 \perp q_3) \simeq (q_1 \perp q_2) \perp q_3$.

(2) $q_1 \perp q_2 \simeq q_2 \perp q_1$.

(3) $\langle a \rangle \perp \langle -a \rangle = \langle a, -a \rangle \simeq \mathbb{H} = 0$ in $W(F)$ for any nonzero element $a \in F$.

(4) $q_1 \otimes q_2 \simeq q_2 \otimes q_1$.

(5) $(q_1 \otimes q_2) \otimes q_3 \simeq q_1 \otimes (q_2 \otimes q_3)$.

(6) $q_1 \otimes (q_2 \perp q_3) \simeq (q_1 \otimes q_2) \perp (q_1 \otimes q_3)$.

It is clear from the condition (3) that a nonzero element in $W(K)$ has an additive inverse since $W(K)$ is generated by 1-dimensional forms $\langle a \rangle$. In fact, $q \perp \mathbb{H} = q$ and $q \otimes \langle 1 \rangle = q$ in $W(F)$. So $\mathbb{H}$ and $\langle 1 \rangle$ can be considered as additive and multiplicative identities on $W(F)$ respectively. Thus $(W(F), \perp, \otimes)$ is a commutative ring with unity. We call it the *Witt ring* of F.

Remark 1.21. $W(\mathbb{C}) \simeq \mathbb{Z}/2\mathbb{Z}$ and $W(\mathbb{R}) \simeq \mathbb{Z}$.

We say that two fields K and L are *Witt equivalent* when $W(K)$ is isomorphic to $W(L)$ as rings. Suppose L is an extension field over $\mathbb{Q}$ of degree two (L is called a quadratic number field). We have the following complete Witt equivalence classification for quadratic number fields.

Theorem 1.22. *(Carpenter and Czogała) There are exactly seven Witt equivalence classes of quadratic number fields, represented by* $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{\pm 2})$, $\mathbb{Q}(\sqrt{\pm 7})$, $\mathbb{Q}(\sqrt{\pm 17})$. *For a square free integer* $n \neq 1$, *the quadratic number field* $\mathbb{Q}(\sqrt{n})$ *is Witt equivalent to* $\mathbb{Q}(\sqrt{d})$, *where* $d = -1$ *if* $n = -1$ *and*

$$d = \begin{cases} sign(n) \cdot 2 & \text{if } |n| \equiv 2, 3, 5, 6 \pmod 8 \\ sign(n) \cdot 7 & \text{if } |n| \equiv 7 \pmod 8 \\ sign(n) \cdot 17 & \text{if } |n| \equiv 1 \pmod 8. \end{cases} \tag{1.11}$$

We have several invariants in $W(K)$. They are very useful for studying quadratic forms. Let $q = \langle a_1, \cdots, a_n \rangle$ be a regular n-ary quadratic form over K. We define the determinant det of a regular quadratic form q to be the square class in K^*/K^{*2} given by $\det(q) = \prod_{i=1}^{n} a_i \cdot K^{*2}$. Equivalent regular quadratic forms have the same determinant. On the other hand, det is not well-defined on $W(K)$. For example, $\mathbb{H} = 2\mathbb{H}$ in $W(K)$, but $\det(\mathbb{H}) = \det\langle 1, -1 \rangle = -1 \cdot K^{*2}$ while $\det(2\mathbb{H}) = \det\langle 1, -1, 1, -1 \rangle = 1 \cdot K^{*2}$. So to get an invariant in $W(K)$ consider the signed determinant which is called the *discriminant*.

Definition 1.23. Let q be a regular n-ary quadratic form over K. Then the discriminant of q is defined to be

$$\operatorname{disc}(q) = (-1)^{\frac{n(n-1)}{2}} \det(q).$$

If q_1 and q_2 are in the same Witt class in $W(K)$, then $\operatorname{disc}(q_1) = \operatorname{disc}(q_2)$ by considering dimensions. So disc is an invariant on $W(K)$. Suppose q_1 and q_2 are in the same Witt class in $W(K)$. Then by the definition of similarity classes, $q_1 = m\mathbb{H} \perp q_2$ for some $m \in \mathbb{Z}$. Thus $\dim(q_1) \equiv \dim(q_2) \pmod 2$. So the map $\dim_0 : W(K) \longrightarrow \mathbb{Z}/2\mathbb{Z}$ defined by $\dim_0(q) = \dim(q) \pmod 2$ is well-defined by the previous argument. The kernel of $\dim_0$ is called the *fundamental ideal*, and is denoted by I_K. Thus $W(K)/I_K \simeq \mathbb{Z}/2\mathbb{Z}$ since $\dim_0$ is onto. Note that I_K is additively generated by binary forms $\langle 1, a \rangle$ (see Proposition 1.5, p. 37 in [11]). The discriminant map $\operatorname{disc} : W(K) \longrightarrow K^*/K^{*2}$ is not necessarily a group homomorphism since $\operatorname{disc}(\langle 1 \rangle + \langle 1 \rangle) = -1 \cdot K^{*2} \neq K^{*2} = \operatorname{disc}\langle 1 \rangle \cdot \operatorname{disc}\langle 1 \rangle$ if -1 is not a square in K^*. On the other hand, if we restrict the domain to I_K, then $\operatorname{disc}|_{I_K}$ is an epimorphism. The kernel of $\operatorname{disc}|_{I_K}$ is I_K^2 (see section 15.2 in [20]). Thus $I_K/I_K^2 \simeq K^*/K^{*2}$.

1.3 Number Fields

A finite extension field of $\mathbb{Q}$ is called a number field.

Definition 1.24. Let R be an integral domain. Let K be a field containing R. Then $s \in K$ is said to be integral over R if s is a root of a monic polynomial $f(x) \in R[x]$. The *integral closure* $O_K(R)$ is the set of all elements in K which are integral over R. In a number field K, we let $O_K = O_K(\mathbb{Z})$, *i.e.*,

$$O_K = \{x \in K \mid x \text{ is integral over } \mathbb{Z}\}.$$

Then O_K is an integral domain, called the ring of integers of K. O_K is integrally closed in K, meaning O_K is the integral closure of O_K in K.

Proposition 1.25. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field with a square free integer $d \in \mathbb{Z}$, $d \neq 1$. Then*

(1) $O_K = \mathbb{Z} \oplus \mathbb{Z} \cdot (\frac{1+\sqrt{d}}{2})$ *if* $d \equiv 1 \pmod 4$.

(2) $O_K = \mathbb{Z} \oplus \mathbb{Z} \cdot \sqrt{d}$ *if* $d \equiv 2, 3 \pmod 4$.

Proof. See Proposition 12.11, p. 189 in [8]. □

In Proposition 1.25, $O_{\mathbb{Q}(\sqrt{d})}$ is a free $\mathbb{Z}$-module of rank $2 = [\mathbb{Q}(\sqrt{d}) : \mathbb{Q}]$. In general, for a given number field K, O_K is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$. That is there are elements $\omega_1, \cdots, \omega_n \in O_K$ for which $O_K = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$, where $n = [K : \mathbb{Q}]$. We call $\omega_1, \cdots, \omega_n$ an *integral basis* of O_K.

Theorem 1.26. *Let K be a number field. Then*

(1) O_K is integrally closed.

(2) O_K is a noetherian ring.

(3) Every nonzero prime ideal P of O_K is maximal.

If an integral domain satisfies the three conditions in Theorem 1.26, then the ring is said to be a *Dedekind domain*. So O_K is a Dedekind ring. On the other

hand, for a given ring R,

$$R \text{ is a Dedekind domain } \iff R \text{ has unique prime ideal decomposition.}$$

Thus in a Dedekind domain R every nonzero ideal I in R has a unique factorization into nonzero prime ideals. Also the prime ideals occurring in the factorization of I are the only prime ideals containing I. Let $p \in \mathbb{Z}$ and let K be a number field. Then,

$$p\,O_K = P_1^{e_1} \cdots P_g^{e_g},$$

where P_i's are distinct prime ideals in O_K and the $e_i > 0$. We call $e_i := e(P_i|p)$ the ramification index of P_i over p. If $e_i > 1$ for some i, then we call p *ramified* in K. We call p *unramified* in K if $e_i = 1$ for all i. By condition (3) of Theorem 1.26, O_K/P_i is a field. In fact, O_K/P_i is an extension field of $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$. The dimension $[O_K/P_i : \mathbb{Z}/p\mathbb{Z}]$ is called the *inertia degree* of P_i over p and is denoted by $f_i := f(P_i|p)$. If p is an unramified prime and $f_i = 1$ for all i, then p is called *completely split* in K.

Theorem 1.27. *Let K be a number field and let $p \in \mathbb{Z}$. Suppose $p\,O_K = P_1^{e_1} \cdots P_g^{e_g}$ where $P_1, \cdots, P_g$ are distinct prime ideals in O_K. Then*

$$\sum_{i=1}^{g} e_i f_i = n, \text{ where } n = [K : \mathbb{Q}].$$

Proof. See Theorem 3, p. 181 in [8]. □

If $K/\mathbb{Q}$ is a Galois extension, all the prime ideals lying over p have the same inertia degree f and the same ramification index e. So we can rewrite the formula in Theorem 1.27 as

$$efg = n, \text{ where } n = [K : \mathbb{Q}]$$

.

Theorem 1.28. *Let $K = \mathbb{Q}(\sqrt{d}\,)$ be a quadratic extension with a square free $d \in \mathbb{Z}$ and let p be a prime number.*

(1) If p is odd and $p \nmid d$, then

$$p\,O_K = \begin{cases} (p, n+\sqrt{d}\,)(p, n-\sqrt{d}\,), & \text{if } d \equiv n^2 \pmod{p}, \\ \text{prime}, & \text{if } d \not\equiv n^2 \pmod{p} \text{ for any } n \in \mathbb{Z}. \end{cases} \tag{1.12}$$

(2) If $p \mid d$, then $p\,O_K = (p, \sqrt{d}\,)^2$.

(3) If d is odd, then,

$$2\,O_K = \begin{cases} (2, 1+\sqrt{d}\,)^2 & \text{if } d \equiv 3 \pmod{4}, \\ (2, \frac{1+\sqrt{d}}{2}\,)(2, \frac{1-\sqrt{d}}{2}\,) & \text{if } d \equiv 1 \pmod{8}, \\ \text{prime} & \text{if } d \equiv 5 \pmod{8}. \end{cases} \tag{1.13}$$

Proof. See Proposition 13.1.3 and Proposition 13.1.4, p. 190 in [8]. □

Let K be a number field and let P be a prime ideal in O_K. Suppose $P \cap \mathbb{Z} = (p)$. The norm $\mathcal{N}(P)$ of the ideal P is defined to be p^f, where $f = f(P|p)$. We define a map $|\ |_P : K \to [0, \infty)$ by $|\,a|_P = (\frac{1}{\mathcal{N}(P)})^{ord_P(aO_K)}$ for nonzero a and we define $|\,0|_P = 0$. Then $|\ |_P$ satisfies the axioms of a non-archimedean valuation. The completion K_P of K with respect to the valuation $|\ |_P$ contains the field $\mathbb{Q}_p$. It is known that $[K_P : \mathbb{Q}_p] = e(P|p)f(P|p)$. The restriction of $|\ |_P$ on K_P to the subfield $\mathbb{Q}_p$ is $|\ |_p^{[K_p:\mathbb{Q}_p]}$ which is usually distinct from but always equivalent to the normalized p-adic valuation $|\ |_p$ on $\mathbb{Q}_p$. The valuation $|\ |_P^{\frac{1}{n_P}}$ with $n_P = e(P|p)f(P|p)$ is the actual extension of $|\ |_P$ to K_P. As we have seen above, a prime ideal P in K induces a non-archimedean valuation. There is a one-to-one correspondence between prime ideals and non-archimedean places. So usually we identify a prime ideal P with $|\ |_P$ and call P a finite prime. In particular, P is called a *dyadic*

prime if $P \bigcap \mathbb{Z} = (2)$. Let K be a number field with $[K : \mathbb{Q}] = n$. Then there are n embeddings (called infinite primes) into $\mathbb{C}$. Suppose there are r real infinite primes and s pairs of complex infinite primes, *i.e.*, $n = r + 2s$. By composing each real infinite prime (complex infinite prime respectively) with the absolute value function on $\mathbb{R}$ (absolute value function from $\mathbb{C}$ into $\mathbb{R}$ respectively) we get $r + s$ infinite places. The set of all nontrivial places ("primes") of a number field K is denoted by Ω_K. Suppose $\sigma_1, \cdots, \sigma_n$ are embeddings of a number field K into $\mathbb{C}$ with $[K : \mathbb{Q}] = n$. Then we define

$$T(\alpha) := \sum_{i=1}^{n} \sigma_i(\alpha) \quad \text{and} \quad N(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha),$$

where $\alpha \in K$. We call $T(\alpha)$ (resp. $N(\alpha)$) *trace* of α (resp. *norm* of α). We also define $N(I)$ of an ideal I in O_K by the ideal generated by elements $N(\alpha)$ for $\alpha \in I$. It is clear that $T(\alpha), N(\alpha) \in \mathbb{Z}$ if $\alpha \in O_K$ since those elements are ± 1 times the coefficients of the irreducible monic polynomial of α in $\mathbb{Z}[x]$. So $N(I) = m\mathbb{Z}$ for a positive integer m. The number m is called the *absolute norm* of the ideal I and is denoted by $\mathcal{N}(I)$. The absolute norm $\mathcal{N}(I)$ is the number of elements in O_K/I. In particular $\mathcal{N}(P) = p^{f(P|p)}$, where $P \cap O_K = (p)$.

The discriminant of n elements $a_1, \cdots, a_n$ of K is defined by

$$D_K(a_1, \cdots, a_n) := \det(\sigma_i a_j)^2.$$

We call the discriminant of an integral basis of O_K the *discriminant of* K (denoted by d_K). The discriminant d_K of K does not depend on the choice of integral basis. If we use the integral basis for the quadratic field $\mathbb{Q}(\sqrt{d}\,)$ exhibited in Proposition 1.25, we obtain

$$d_K = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2, 3 \pmod 4, \end{cases} \tag{1.14}$$

where d is a square free element in $\mathbb{Z}$.

Theorem 1.29. *Suppose p is a prime in $\mathbb{Z}$ which ramifies in a number field K. Then $p \mid d_K$.*

Proof. See p. 72 in [13]. □

2. Hilbert Symbol Equivalence and Arf Equivalence

2.1 Local Root Numbers

Root numbers come from a functional equation of Artin L-functions, which are generalizations of the Dedekind zeta function.

Definition 2.1. Let K be a number field. The Dedekind zeta function $\zeta_K(s)$ of K is defined by

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where a_n is a number of non-zero ideals in O_K of norm n and s is a complex number with $Re(s) > 1$.

When $K = \mathbb{Q}$, $\zeta_{\mathbb{Q}}(s)$ is the Riemann zeta function. The Dedekind zeta function can be extended to a meromorphic function. That is, $\zeta_K(s)$ can be defined for all complex numbers by accepting finitely many simple poles. The Dedekind zeta function has a functional equation relating the value at s and to the value at $1-s$. It involves the gamma function which is a generalization of the factorial function.

Definition 2.2. The gamma function is defined by

$$\Gamma(s) = \int_0^{\infty} e^{-x} x^{s-1} dx,$$

where s is a complex number with $Re(s) > 0$.

Integrating by parts shows that $\Gamma(s) = (s-1)\Gamma(s-1)$ for $\mathrm{Re}(s) > 0$. Putting $s = n =$ a positive integer, this implies that $\Gamma(n) = (n-1)!\Gamma(1)$. So $\Gamma(n) = (n-1)!$ for $n = 1, 2, 3, \cdots$, since

$$\Gamma(1) = \int_0^{\infty} e^{-x} dx = \lim_{t \to \infty} [-e^{-x}]_0^t = 1.$$

The relation $\Gamma(s) = (s-1)\Gamma(s-1)$ for $\mathrm{Re}(s) > 0$ shows that $\Gamma(s)$ can be extended for all $s \in \mathbb{C}$ to a function having simple poles of 0 and the negative integers. The

following functional equation of the Dedekind zeta function holds:

$$\begin{aligned}&[\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})]^{r_1(K)}[(2\pi)^{1-s}\Gamma(s)]^{r_2(K)}\zeta_K(s) = \\ &|d_K|^{\frac{1}{2}-s}[\pi^{\frac{s-1}{2}}\Gamma(\frac{1-s}{2})]^{r_1(K)}[(2\pi)^{s}\Gamma(1-s)]^{r_2(K)}\zeta_K(1-s),\end{aligned} \tag{2.15}$$

where d_K is the discriminant of K, $r_1(K)$ is the number of real embeddings of K and $r_2(K)$ is the number of pairs of complex embeddings of K. To get a nice functional equation we define the generalized Dedekind zeta function Z_K by

$$Z_K(s) = |d_K|^{\frac{2s-1}{4}}[\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})]^{r_1(K)}[(2\pi)^{1-s}\Gamma(s)]^{r_2(K)}\zeta_K(s). \tag{2.16}$$

It is clear that $Z_K(s)$ determines $\zeta_K(s)$ and vice versa for a given K. Then the equation 2.15 can be restated as follows:

$$Z_K(s) = Z_K(1-s). \tag{2.17}$$

There is an Artin L-series $L(s,\rho)$ for a representation $\rho : \mathrm{Gal}\,(\overline{K}|K) \longrightarrow \mathbf{GL}_n(\mathbb{C})$. We do not give its somewhat complicated definition here, but merely state that if ρ is the trivial 1-dimensional representation, then $L(s,\rho) = \zeta_K(s)$. Just as $\zeta_K(s)$ has a "generalized" version $Z_K(s)$ which satisfies a nice functional equation, so $L(s,\rho)$ has a generalized version, $\Lambda(s,\rho)$ that satisfies

$$\Lambda(s,\rho) = W(\rho)\cdot\Lambda(1-s,\bar{\rho}), \tag{2.18}$$

where $W(\rho) \in \mathbb{C}^*$. We call $W(\rho)$ the global root number. The global root number is a complex number of absolute value 1. Now we are in a position to define *local root numbers*. Let P be a place of K. Consider the completion K_P of K at P. The local absolute Galois group $G(K_P) := \mathrm{Gal}\,(\overline{K_P}|K_P)$ can be considered to be a subgroup of $G(K)$ which is determined only up to conjugation in $G(K)$. That is, $G(K_P)$ can be thought of a conjugacy class in $G(K)$. Choose any one of those subgroups and temporarily call it H. Restricting ρ to H defines a representation

of H. Replacing H by a conjugacy subgroup leads to a representation of H that is isomorphic to the representation constructed above. In this sense $\rho|_H$ does not depend on which subgroup H is chosen. We will denote $\rho|_H$ by ρ_P. Deligne has shown how to associate a complex number $W(\rho_P)$ to ρ_P. Conjecturally there is "local Artin L-series" satisfying a local version of (2.18) in which $W(\rho_P)$ replaces $W(\rho)$. While this remains a conjecture, the complex numbers $W(\rho_P)$ are known to exist. There is a relation between $W(\rho)$ and $W_P(\rho_P)$ as follows:

$$W(\rho) = \prod_{P \in \Omega_K} W_P(\rho_P).$$

Theorem 2.3. *(Fröhlich-Queyrut) If K/F is a finite Galois extension of number fields and ρ is a real orthogonal representation of* $\mathrm{Gal}\,(K/F)$*, then $W(\rho) = 1$.*

Let K be a number field and let $a \in K$. We define a real representation $\rho_a : \mathrm{Gal}\,(\overline{K}|K) \longrightarrow \mathbf{GL}_1(\mathbb{C})$ by $\rho_a(g) = \frac{g(\sqrt{a})}{\sqrt{a}}$ for every $g \in \mathrm{Gal}\,(\overline{K}|K)$. By the previous argument we have only one local root number $W_P(\rho_a)$ for a given place P of K. So we can define a map $r_P : K_P^*/K_P^{*2} \longrightarrow \mathbb{C}^*$ (called a "local root number function") by $r_P(a) := W_P(\rho_a)$. The local square-class group K_P^*/K_P^{*2} for a place P is an $\mathbb{F}_2$-vector space with a finite dimension. They are classified as follows: (See Theorem 2.22, p. 161 in [11])

$$\dim_{\mathbb{F}_2} K_P^*/K_P^{*2} = \begin{cases} 0 & \text{if } P \text{ is complex,} \\ 1 & \text{if } P \text{ is real,} \\ 2 & \text{if } P \text{ is finite and non-dyadic,} \\ 2 + [K_P : \mathbb{Q}_2] & \text{if } P \text{ is dyadic.} \end{cases} \tag{2.19}$$

Definition 2.4. Let K be a local field, i.e., $\mathbb{R}$ or $\mathbb{C}$, or the field $\mathbb{Q}_p$ of p-adic numbers. Let a and b be nonzero elements of K. We define the *Hilbert symbol*

$(a,b)_K$ by

$$(a,b)_K = \begin{cases} 1 & \text{if } \langle a,b,-1\rangle \text{ is isotropic,} \\ -1 & \text{otherwise.} \end{cases} \tag{2.20}$$

Theorem 2.5. *Let K be a local field. Then the following hold for the Hilbert symbol. ([22], p. 54)*

(1) $(a,b)_K = (b,a)_K$ for $a,b \in K^*$.

(2) $(a,-a)_K = (a,1-a)_K = 1$ for $a \in K$ with $a \neq 0,1$.

(3) $(ab,c)_K = (a,c)_K(b,c)_K$ for $a,b,c \in K^*$.

(4) $(a,b)_K = 1$ for all $a,b \in K^*$ if $K = \mathbb{C}$.

(5) $(a,p)_K = (\frac{a_0}{p})$ for $a \in \mathbb{Z}_p^*$, where $K = \mathbb{Q}_p$ with $p \neq 2$, $a_0 \in \mathbb{Z}$, $a \equiv a_0$ mod $p\mathbb{Z}_p$ and $(\frac{a_0}{p})$ is the Legendre symbol.

(6) Suppose $K = \mathbb{Q}_2$ and $a,b \in \mathbb{Z}_2^*$. Then

$$(a,b)_2 = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}} \text{ and } (a,2)_2 = (-1)^{\frac{a^2-1}{8}}$$

(7) If $(x,a)_K = 1$ for all $x \in K^*$, then $a \in K^{*2}$.

Let K be a number field with a prime ideal P in O_K. Then we denote $(a,b)_{K_P}$ by $(a,b)_P$ for $a,b \in K_P^*$. The Hilbert symbol $(\ ,\ )_P$ on the local-square class group K_P^*/K_P^{*2} is bilinear by Theorem 2.5.

Proposition 2.6. *Let u and v be units in $\mathbb{Q}_p$ where $p \neq 2$. Then*

(1) $(p,u)_p = -1$ where u is a non-square unit in $\mathbb{Q}_p$.

(2) $(u,v)_p = 1$.

Proof. See 6-6-4, p. 251 in [22]. □

Theorem 2.7. *(Hilbert reciprocity Law) Let a and b be nonzero elements of an algebraic number field K. Then $(a,b)_P$ is 1 for almost all primes P, and*

$$\prod_{P \in \Omega_K} (a,b)_P = 1,$$

where Ω_K is the set of all primes of K. The product is also one if we exclude all complex archimedean places.

Proof. See 71:18, p. 201 in [15]. □

Definition 2.8. Let (V, B) be an inner product over a number field K, with a regular quadratic form $q = \langle a_1, \cdots, a_n \rangle$ and let P be a prime (finite or infinite) in a number field K. We define the *Hasse invariant* $h_P(q)$ of the quadratic space (V, B) by

$$h_P(q) := \prod_{i<j} (a_i, a_j)_P,$$

and we define $h_P(q) = 1$ for every one dimensional regular quadratic form q.

Then we can easily see that

$$h_P(q_1 \perp q_2) = h_P(q_1) h_P(q_2) (\det(q_1), \det(q_2))_P.$$

An easy computation tells us $h_\infty(2\mathbb{H}) = -1$ and $h_\infty(\mathbb{H}) = 1$, where ∞ represents any real infinite prime of K. Therefore h_P is not well defined on the Witt group. To remedy this we define *stable Hasse-Witt invariant* c_P.

Definition 2.9. [5] Let (V, B) be an inner product space with a quadratic form q over a number field K and let P be a prime (finite or infinite) in K. The stable Hasse-Witt invariant $c_p(q)$ is defined as follows:

$$c_P(q) := \begin{cases} h_P(q) & \text{if } \dim V \equiv 0, 1 \pmod 8 \\ h_P(q)(-1, -\det(q))_P & \text{if } \dim V \equiv 2, 3 \pmod 8 \\ h_P(q)(-1, -1)_P & \text{if } \dim V \equiv 4, 5 \pmod 8 \\ h_P(q)(-1, \det(q))_P & \text{if } \dim V \equiv 6, 7 \pmod 8 \ . \end{cases} \tag{2.21}$$

Then $c_P(q)$ depends only on the similarity class of q (See Lemma 12.8, p. 81 in [19]). Let q be a Witt class in $W(K)$. It is known that

(1) $c_P(q) = 1$ for almost all primes.

(2) $c_P(q) = 1$ for all complex primes.

(3) $\prod_{P\in\Omega} c_P(q) = 1$, where Ω is the set of all primes (=nontrivial places) of K.

Suppose F is a finite separable extension of K. Then the trace form of the extension is the symmetric K-bilinear form

$$\mathrm{Tr}_{F/K} : F \times F \longrightarrow K$$

defined by $\mathrm{Tr}_{F/K}(x, y) = \mathrm{Tr}_{F/K}(xy)$. Then we let $\langle F\rangle$ denote Witt class of the trace form. Let $\sigma \in F^*$. We define $\langle F_\sigma\rangle \in W(K)$ to be the Witt class of the trace form B_σ which is defined as

$$B_\sigma(x, y) = \mathrm{Tr}_{F/K}(\sigma xy).$$

B_σ is called a "*scaled trace form*". Then clearly $\langle F_\sigma\rangle = \langle F\rangle$ if $\sigma \in (F^*)^2$. For each nonzero element a in a local field K with a prime P, we can define a quadratic character $\lambda_a : K^* \longrightarrow \mathbb{Z}/2\mathbb{Z}$ by $\lambda_a(x) = (a, x)_P$.

Theorem 2.10. *Let F be a number field and let P be a prime ideal in O_F with $P \cap \mathbb{Z} = (p)$. Then*

$$r_P(a) = (N(a), d_F)_p h_p(\langle F_a\rangle) h_p(\langle F\rangle) r_p(N(a)),$$

where $a \in F_P^*/F_P^{*2}$.

Proof. See Lemma 2.6 in [5]. □

Corollary 2.11. *(Conner-Yui)*

(1) If a rational prime q is unramified in $\mathbb{Q}(\sqrt{n}\,)$, then $r_p(q) = 1$.

(2) If $q \equiv 1 \pmod 4$, then $r_p(q) = 1$ for all primes in $\mathbb{Z}$.

(3) If $q \equiv 3 \pmod 4$, then $r_q(q) = -i$, $r_2(q) = i$, and $r_p(q) = 1$ otherwise.

(4) $r_p(2) = 1$ *for all primes* p *in* $\mathbb{Z}$.

(5) $r_2(-1) = 1$, $r_\infty(-1) = -i$, *and* $r_p(-1) = 1$ *for all odd primes* p

Proof. See Lemma 4.1, Lemma 4.3, and Lemma 4.4 in [5]. □

Here is another approach to get local root numbers. Let α be a continuous linear representation of a local field K_P^* into $\mathbb{C}^*$, where $P \cap \mathbb{Z} = (p)$. Then the set U of units in O_{K_P} is a compact subset of K_P^*. Then the subgroups $1+P^m$, where $m \geq 0$, are a fundamental system of neighborhoods of a unit 1 in U. So $\alpha(1+P^m) = 1$ for some m. Let $m = \inf\{n \,|\, \alpha(1+P^n) = 1, n \geq 0\}$. We call $f_\alpha := P^m$ the *conductor* of α. We define $f_\alpha = O_{K_P}$ if $m = 0$. The character α is called *unramified* if $\alpha(U) = 1$. We define another ideal which is called the *different* of a number field F. Let F and K be number fields with $K \subset F$. Suppose I is an ideal of O_F. Let $I^* := \{x \in F \,|\, \mathrm{Tr}\,(xI) \subseteq O_K\}$. Then $(I^*)^{-1} := \{x \in F \,|\, xI^* \subseteq O_F\}$ is called the *different* of I and is denoted by $D_{F/K}(I)$. In particular, we call $D_{F/K} := D_{F/K}(O_F)$ the different of K over F. If the base field K is the field of rational numbers, then we call $D_{F/\mathbb{Q}}$ the *absolute different* of the field F and denote it by D_F. If the base field K is a p-adic field $\mathbb{Q}_p$ and F is an extension field of $\mathbb{Q}_p$, then $D_{F/\mathbb{Q}_p}$ is called the *local absolute different* of the field F and is denoted by D_F. In general, the different $D_{F/K}$ is an ideal of O_F ([22], p. 110).

Proposition 2.12. *Let* F *and* K *be number fields with* $K \subset F$. *Then*

(1) $\{1, \alpha, \cdots, \alpha^{n-1}\}$ *is an integral basis of* $O_F \Longleftrightarrow D_{F/K} = f'(\alpha)O_F$,

where $f(x)$ *is an irreducible monic polynomial of* α *in* $O_K[x]$.

(2) Let Q *be an ideal of* O_F *with* $Q \cap O_K = P$. *Then* $Q \,|\, D_{F/K} \Longleftrightarrow e(Q|P) > 1$.

Proof. See p112 in [22] and p120 in [13]. □

Let F be a finite extension of $\mathbb{Q}_p$, where p is a prime. We define an additive character $\psi_F : F \longrightarrow \mathbb{C}^*$ which is the composition of the following maps,

$$F \xrightarrow{\alpha} \mathbb{Q}_p \xrightarrow{\beta} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\gamma} \mathbb{Q}/\mathbb{Z} \xrightarrow{\delta} \mathbb{R}/\mathbb{Z} \xrightarrow{\epsilon} \mathbb{C}^*,$$

where α is the trace map, β is the canonical surjection, γ is the canonical injection, i.e., $\gamma(a_{-n}p^{-n} + a_{-n+1}p^{-n+1} + \cdots + a_{-1}p^{-1} + \mathbb{Z}_p) = \sum_{i=1}^{n} a_{-i}p^{-i} + \mathbb{Z}$, where each coefficient is an element of $\{0, 1, \cdots, p-1\}$, δ is a canonical injection and $\epsilon(x+\mathbb{Z}) = e^{2\pi x i}$.

Theorem 2.13. *(Tate, [21])*

Let F be a number field.

(1) Suppose P is a finite place of F. Then

$$r_P(\alpha) = \frac{1}{\sqrt{\mathcal{N} f_\alpha}} \sum_{x \in U_{F_P} \mod {}^* f_\alpha} \overline{\alpha}\,(d^{-1}x)\,\psi_{F_P}(d^{-1}x),$$

where $U_{F_P} := O_{F_P}^*$ is local unit groups, $dO_{F_P} = f_\alpha D_{F_P}$, ψ_{F_P} is the map defined above, and $x \in U_{F_P} \mod {}^* f_\alpha$ means x is a coset of $1 + f_\alpha$ and $1 + f_\alpha = U_{F_P}$ if $f_\alpha = O_{F_P}$.

(2) Suppose P is complex. Then $r_P(\alpha) = 1$.

(3) Suppose P is real. Then

$$r_P(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is trivial.} \\ -i & \text{otherwise} \end{cases}$$

Theorem 2.14. *For $a, b \in K_P^*/K_P^{*2}$,*

$$r_P(ab) = (a, b)_P \cdot r_P(a) \cdot r_P(b).$$

Proof. See Corollary 2, p. 126 in [21]. □

2.2 Hilbert Symbol Equivalence

Let K and L be Witt equivalent number fields with a ring isomorphism ϕ. Then ϕ maps I_K^m to I_L^m for any m. Thus ϕ induces group isomorphisms

$$t_\phi : I_K/I_K^2 \longrightarrow I_L/I_L^2 \quad \text{and} \quad u_\phi : I_K^2/I_K^3 \longrightarrow I_L^2/I_L^3.$$

Combining t_ϕ with the multiplication map $I_K/I_K^2 \times I_K/I_K^2 \longrightarrow I_K^2/I_K^3$ yields a commutative diagram:

$$\begin{array}{ccc} I_K/I_K^2 \times I_K/I_K^2 & \longrightarrow & I_K^2/I_K^3 \\ {\scriptstyle t_\phi \times t_\phi}\downarrow & & {\scriptstyle u_\phi}\downarrow \\ I_L/I_L^2 \times I_L/I_L^2 & \longrightarrow & I_L^2/I_L^3 \end{array} \tag{2.22}$$

The discriminant map $\mathrm{disc}_K : I_K/I_K^2 \longrightarrow K^*/K^{*2}$ is an isomorphism,

where $\mathrm{disc}_K(\langle 1, a\rangle + I_K^2) = -a$. So the above diagram can be rephrased as follows:

$$\begin{array}{ccc} K^*/K^{*2} \times K^*/K^{*2} & \longrightarrow & I_K^2/I_K^3 \\ {\scriptstyle t\times t}\downarrow & & {\scriptstyle u}\downarrow \\ L^*/L^{*2} \times L^*/L^{*2} & \longrightarrow & I_L^2/I_L^3, \end{array} \tag{2.23}$$

where $t = \mathrm{disc}_L \circ t_\phi \circ \mathrm{disc}_K^{-1}$ and $u = u_\phi$.

Theorem 2.15. *(Harrison's Criterion) Let K and L be number fields. Then the following are equivalent:*

(1) $W(K) \simeq W(L)$ as rings.

(2) There are group isomorphisms $t : K^*/K^{*2} \longrightarrow L^*/L^{*2}$ and $u : I_K^2/I_K^3 \longrightarrow I_L^2/I_L^3$ such that the diagram (2.23) commutes.

(3) There is a group isomorphism $t : K^*/K^{*2} \longrightarrow L^*/L^{*2}$ such that $t(-1) = -1$ and a binary form $\langle a, b\rangle$ represents 1 over K if and only if $\langle ta, tb\rangle$ represents 1 over L.

Proof. See p. 370 in [17]. □

Definition 2.16. Let K and L be number fields. Suppose there is a pair (T, t), where $t : K^*/K^{*2} \longrightarrow L^*/L^{*2}$ is a group isomorphism between square classes of K and L, and $T : \Omega_K \longrightarrow \Omega_L$ is a bijection between the sets Ω_K and Ω_L of nontrivial places with

$$(a, b)_P = (ta, tb)_{TP}$$

for all $a, b \in K^*/K^{*2}$ and all $P \in \Omega_K$. Then the two number fields K and L are called *Hilbert symbol equivalent.*

Theorem 2.17. *Number fields K and L are Hilbert symbol equivalent if and only if they are Witt equivalent.*

Proof. See Theorem 1, p. 377 in [17]. □

2.3 Refinements of Bilinear Forms on $\mathbb{F}_2$

Throughout this section, a bilinear space is an n dimensional vector space over the field $\mathbb{F}_2$ of two elements. Fix a basis $\{v_1, \cdots, v_n\}$ of V and let $M_{B,\{v_1,\cdots,v_n\}} = (B(v_i, v_j))$. Choosing a different basis replaces $M_{B,\{v_1,\cdots,v_n\}} = (B(v_i, v_j))$ by a congruent matrix.

Lemma 2.18. *Let B be a non-degenerate symmetric bilinear form on a vector space of dimension n over $\mathbb{F}_2$. Then*
(1) If n is odd, then $M_B \simeq I_n$.
(2) If n is even, then either $M_B \simeq I_n$ or $M_B \simeq \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Proof. See Theorem 19 and 20 in [9]. □

We say that a bilinear space B is type II when B is totally isotropic and B is type I otherwise.

Definition 2.19. [16] A classical refinement of a bilinear space (V, B) over $\mathbb{F}_2$ is a map $q : V \longrightarrow \mathbb{F}_2$ satisfying

$$q(v + w) = B(v, w) + q(v) + q(w) \tag{2.24}$$

for all $v, w \in V$.

Clearly $q(0) = 0$. When B has a classical refinement then putting $w = v$ in (2.24) shows $B(v, v) = 0$, so B has type II. Thus type I spaces do not have classical refinements. To get refinements for type I spaces, we modify the situation. Let $\theta : \mathbb{F}_2 \longrightarrow \mathbb{C}^*$ be a map defined by $\theta(0) = 1$, $\theta(1) = -1$ and let $\beta = \theta \circ B$.

Definition 2.20. [16] For a given bilinear space (V, B) a refinement is a map $q : V \longrightarrow \mathbb{C}^*$ that satisfies

$$q(v + w) = \beta(v, w) \cdot q(v) \cdot q(w)$$

for all $v, w \in V$.

Theorem 2.21. *Every nondegenerate bilinear space (V, B) of dimension n over $\mathbb{F}_2$ has exactly 2^n refinements.*

Proof. See Theorem 2, p. 384 in [16]. □

Remark 2.22. [16] For a given refinement q,

(1) $q(0) = 1$.

(2) $q(v)^2 = \beta(v, v)$.

(3) $q(v) \in \{\pm 1, \pm i\}$. This follows from (2).

Remark 2.23. Here is a way to obtain all the other refinements from any particular refinement q for a nondegenerate bilinear space (V, B). Let $w \in V$. We define a map $q_w : V \longrightarrow \mathbb{C}^*$ by

$$q_w(v) = \beta(v, w) \cdot q(v)$$

Then q_w is a refinement and $q_w \neq q_{w'}$ if $w \neq w'$ in V.

Proof. First we show q_w is a refinement.

$$\begin{aligned} q_w(v+v') &= \beta(v+v', w) \cdot q(v+v') \\ &= \beta(v,w) \cdot \beta(v',w) \cdot \beta(v,v') \cdot q(v) \cdot q(v') \\ &= \beta(v,v') \cdot \beta(v,w) \cdot q(v) \cdot \beta(v',w) \cdot q(v') \\ &= \beta(v,v') \cdot q_w(v) \cdot q_w(v'). \end{aligned}$$

So q_w is a refinement. We show that $q_w \neq q_{w'}$ for any two different elements w and w' in V. Suppose $w \neq w'$. Then $w - w' \neq 0$. So there exists an element $v \in V$ such that $\beta(v, w-w') = -1$ since B is nondegenerate. Then

$$\frac{q_w(v)}{q_{w'}(v)} = \frac{\beta(v,w)q(v)}{\beta(v,w')q(v)} = \beta(v, w-w') = -1$$

Therefore $q_w(v) \neq q_{w'}(v)$, so $q_w \neq q_{w'}$. □

2.4 Arf Equivalence

Arf showed in an equivalent formulation that two classical refinements q and q' for a type II space are isometric if and only if $\sum_{i=1}^{m} q(v_i)q(w_i) = \sum_{i=1}^{m} q'(v_i)q'(w_i)$, where $\{v_1, w_1, \cdots, v_m, w_m\}$ is a symplectic basis. The sum $\sum_{i=1}^{m} q(v_i)q(w_i)$ was its original "Arf invariant". We will produce a new-style Arf invariant for multiplicative refinements of a bilinear space whether type I or type II. We want to call this new invariant "Arf invariant". So we use the terminology "Ur-Arf" for Arf's original invariant. As we have seen in the previous section, there is no classical refinements for type I spaces.

Definition 2.24. [16] The *Arf invariant* of (V, B, q) is

$$Arf(V, B, q) = 2^{-\frac{n}{2}} \sum_{v \in V} q(v),$$

where n is the degree of V over $\mathbb{F}_2$.

If (V, B) is fixed, then $Arf(q)$ is also used for $Arf(V, B, q)$. Let (V, B) be an inner product space over $\mathbb{F}_2$. The adjoint map

$$adj : V \longrightarrow \mathrm{Hom}(V, \mathbb{F}_2)$$

defined by $adj_w(v) = B(v, w)$ is an isomorphism since B is nondegenerate. Consider a map $\lambda : V \longrightarrow \mathbb{F}_2$ defined by $\lambda(v) = B(v, v)$. Then $\lambda \in \mathrm{Hom}(V, \mathbb{F}_2)$. So there exists a unique vector $c \in V$ such that $adj_c = \lambda$, i.e., $B(v, c) = B(v, v)$ for all $v \in V$. We call $c := c(B)$ the *canonical vector* of (V, B). If ϕ is an isometry between inner product spaces (V, B) and (V, B') and c is the canonical vector of (V, B), then $\phi(c) = c(B')$. Suppose an inner product space (V, B) is a type II space and let c be the canonical vector. Then $B(v, c) = B(v, v) = 0$ for all $v \in V$. So $c = 0$ since B is nondegenerate.

Lemma 2.25. *Let q be a refinement of an inner product space (V, B) and let c be the canonical vector of (V, B). Then the following are satisfied.*

(a) $\sum_{v \in V} \beta(v, w) = 0$ *for any nonzero* $w \in V$.

(b) $Arf(q)^2 = q(c)$.

(c) $Arf(q)^4 = \beta(c, c) = (-1)^{\dim(V)}$.

Proof. See Lemma 1, p. 387 in [16]. □

From (c) of Lemma 2.25 it is clear $\mathrm{Arf}(q)$ is an eighth root of unity and is a primitive eighth root of unity if and only if $\dim(V)$ is odd.

Theorem 2.26. *Two inner product spaces (V, B, q) and (V', B', q') are isometric if and only if*

$$\dim(V) = \dim(V'),$$

$$type(V, B) = type(V', B'),$$

$$Arf(V, B, q) = Arf(V', B', q').$$

Proof. See Theorem 4, p. 388 in [16]. □

Definition 2.27. [16] Let K and L be number fields and let the map T be a bijection between the set Ω_K of places of K and the set Ω_L of places of L. Two fields K and L are called *Arf equivalent* if

$$\dim[K_P^*/K_P^{*2}] = \dim[L_{TP}^*/L_{TP}^{*2}],$$

$$\text{type}[(\ ,\ )_P] = \text{type}[(\ ,\ )_{TP}],$$

$$\text{Arf}\,[r_P] = \text{Arf}\,[r_{TP}].$$

Let K be a number field with a place P. Then

$$(a, a)_P = (a, -1)_P$$

for every $a \in K_P^*/K_P^{*2}$. So by (7) of Theorem 2.5

$$\text{the space } K_P^*/K_P^{*2} \text{ is type II } \iff -1 \in K_P^{*2}.$$

We can also see for two number fields to be Arf equivalent any non-dyadic place in one field cannot be matched with a dyadic place in the other field by the dimension argument. (see section 2.1)

Theorem 2.28. *Let K and L be number fields. If K and L are Arf equivalent, then they are Witt equivalent.*

Proof. See Theorem 5, p. 391 in [16]. □

Corollary 2.29. *There are at least seven Arf equivalence classes of quadratic number fields.*

Proof. It is clear by Theorem 1.22 and Theorem 2.28. □

So the natural question is " how many Arf equivalence classes exist in quadratic number fields?". We study this question in the next chapter.

3. Main Results

In this chapter, we find some local root numbers in quadratic extension fields over p-adic completions $\mathbb{Q}_p$ for a rational prime p.

3.1 Some Computations

In this section we always assume $\mathbb{F}_{p^2} \cong \mathbb{F}_p[\theta] \cong \mathbb{F}_p[x]/\langle x^2 - c\rangle$, where $c \notin (\mathbb{F}_p^*)^2$ and θ is a root of $x^2 - c$ in $\overline{\mathbb{F}_p}$.

Lemma 3.1. *Let p be an odd prime in $\mathbb{Z}$. Then every element in $\mathbb{F}_p$ is a square in the degree two extension $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$.*

Proof. It is enough to show that c is a square in $\mathbb{F}_{p^2}$. Clearly $c = \theta^2 \in (\mathbb{F}_p[\theta]^*)^2$. It is known that there is only one equivalence class of degree two extensions over $\mathbb{F}_p$ since $x^{p^2-1} = 1$ for every element x in any degree two extension of $\mathbb{F}_p$. Therefore $c \in (\mathbb{F}_{p^2}^*)^2$. □

Suppose $p \in \mathbb{Z}$ is an odd prime. We define a trace map $\mathrm{Tr} : \mathbb{F}_p[\theta] \longrightarrow \mathbb{F}_p$ by $\mathrm{Tr}(x) = x + x^p$. Then $\mathrm{Tr}(\theta) = 0$ since $\theta^p = \theta^{p-1} \cdot \theta = (\theta^2)^{\frac{p-1}{2}} \cdot \theta = c^{\frac{p-1}{2}} \cdot \theta = -\theta$. So $\mathrm{Tr}(a + b\theta) = \mathrm{Tr}(a) + b\mathrm{Tr}(\theta) = 2a$ for $a, b \in \mathbb{F}_p$. Now we consider the function $s : \mathbb{F}_{p^2} \longrightarrow \{-1, 0, 1\}$ defined by $s(x) = 1$ if $x \in (\mathbb{F}_{p^2}^*)^2$, $s(x) = -1$ if $x \notin (\mathbb{F}_{p^2})^2$, and $s(0) = 0$.

Lemma 3.2. *Suppose p is an odd prime in $\mathbb{Z}$. Then*

(1) $\sum_{x \in \mathbb{F}_{p^2}^*, \mathrm{Tr}(x)=0} s(x) = -(p-1)$ *and* $\sum_{x \in \mathbb{F}_{p^2}^*, \mathrm{Tr}(x)=j} s(x) = 1$ *for each* $j \in \mathbb{F}_p^*$ *if* $p \equiv 1 \pmod 4$.

(2) $\sum_{x \in \mathbb{F}_{p^2}^*, \mathrm{Tr}(x)=0} s(x) = p - 1$ *and* $\sum_{x \in \mathbb{F}_{p^2}^*, \mathrm{Tr}(x)=j} s(x) = -1$ *for each* $j \in \mathbb{F}_p^*$ *if* $p \equiv 3 \pmod 4$.

Proof. First we show that $\sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=j} s(x) = \sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=j'} s(x)$ where $j \neq j'$ in $\mathbb{F}_p^*$. There is an element $t \in \mathbb{F}_p^*$ such that $j' = tj$ since $j\mathbb{F}_p^* = \mathbb{F}_p^*$. Let $C_j = \{x \in \mathbb{F}_{p^2}^* | \,\mathrm{Tr}\,(x) = j\}$ and let $C_{j'} = \{x \in \mathbb{F}_{p^2}^* | \,\mathrm{Tr}\,(x) = j'\}$. Suppose α_j is in C_j. Then $\mathrm{Tr}\,(t\alpha_j) = t\mathrm{Tr}\,(\alpha_j) = tj = j'$. So $t\alpha_j \in C_{j'}$. Let $\alpha_{j'} \in C_{j'}$. Then $\mathrm{Tr}\,(t^{-1}\alpha_{j'}) = t^{-1}\mathrm{Tr}\,(\alpha_{j'}) = t^{-1}j' = j$. Thus $t^{-1}\alpha_{j'} \in C_j$. So there is a one-to-one correspondence between elements in C_j and elements in $C_{j'}$ by the mapping $\phi : C_j \longrightarrow C_{j'}$ defined by $\phi(\alpha_j) = t\alpha_j$. Therefore $|C_j| = |C_{j'}|$. Moreover $s(t\alpha_j) = s(\alpha_{j'})$ since $t \in (\mathbb{F}_{p^2}^*)^2$ by the Lemma 3.1. Therefore $\sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=j} s(x) = \sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=j'} s(x)$.

(1) Suppose $p \equiv 1 \pmod 4$. We show θ is a non-square in $\mathbb{F}_{p^2}$. Assume $\theta = (a+b\theta)^2$ for some $a, b \in \mathbb{F}_p$. This yields the equations $a^2 + cb^2 = 0$ and $2ab = 1$. So a and b are non-zero elements in $\mathbb{F}_p$. By combining two equations we get $c = -2a^4 \in (\mathbb{F}_p^*)^2$ since -2 is a square in $(\mathbb{F}_p^*)^2$ by the Lemma 3.1. This contradicts c is a non-square element in $\mathbb{F}_p$. So $s(\theta) = -1$. This implies $s(i\theta) = -1$ for any $i \in \mathbb{F}_p^*$ by the Lemma 3.1. Thus $\sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=0} s(x) = \sum_{i=1}^{p-1} s(i\theta) = \sum_{i=1}^{p-1}(-1) = -(p-1)$. On the other hand, $\mathbb{F}_{p^2}^*$ is a multiplicative cyclic group of an even order. So $\sum_{x\in\mathbb{F}_{p^2}^*} s(x) = 0$. Thus

$$\begin{aligned} 0 &= \sum_{x\in\mathbb{F}_{p^2}^*} s(x) \\ &= \sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=0} s(x) + \sum_{j=1}^{p-1}\{\sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=j} s(x)\} \\ &= -(p-1) + (p-1)\{\sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=1} s(x)\}. \end{aligned}$$

So we get $\sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=j} s(x) = 1$ for $j = 1, \cdots p-1$.

(2) Suppose $p \equiv 3 \pmod 4$. In this case -1 can be taken for c. i.e., $\theta^2 = -1$. Then we get $s(\theta) = 1$ from the following computation

$$1 = s((1+\theta)^2) = s(1 + 2\theta + \theta^2) = s(2\theta) = s(\theta)$$

since $2 \in (\mathbb{F}_{p^2}^*)^2$ by the Lemma 3.1. So $s(j\theta) = 1$ for any $j \in \mathbb{F}_p^*$ by the Lemma 3.1. Thus $\sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=0} s(x) = \sum_{j=1}^{p-1} s(j\theta) = \sum_{j=1}^{p-1} 1 = p-1$. On the other hand, $\mathbb{F}_{p^2}^*$ is a multiplicative cyclic group of even order. So $\sum_{x\in\mathbb{F}_{p^2}^*} s(x) = 0$. Thus

$$\begin{aligned} 0 &= \sum_{x\in\mathbb{F}_{p^2}^*} s(x) \\ &= \sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=0} s(x) + \sum_{j=1}^{p-1}\{\sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=j} s(x)\} \\ &= (p-1) + (p-1)\{\sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=1} s(x)\}. \end{aligned}$$

So we get $\sum_{x\in\mathbb{F}_{p^2}^*,\mathrm{Tr}\,(x)=j} s(x) = -1$ for $j = 1, \cdots p-1$.

□

Lemma 3.3. *A quadratic Gauss sum* $G_a := \sum_{t=1}^{p-1}(\frac{t}{p})\zeta^{at}$ *is classified as follows:*

$$G_a = \begin{cases} (\frac{a}{p})\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ i(\frac{a}{p})\sqrt{p} & \text{if } p \equiv 3 \pmod 4, \end{cases} \tag{3.25}$$

where $(\frac{t}{p})$ *is the Legendre symbol and* ζ *is a primitive* p^{th} *roof of unity, i.e.* $\zeta = e^{\frac{2\pi i}{p}}$.

Proof. See p. 71 and p. 75 in [8]. □

Let p be an odd prime. Then by Theorem 1.28 and Theorem 1.29 , p is ramified in $\mathbb{Q}(\sqrt{ep})$ and $(p) = P^2 = (p,\Pi)^2$, where $\Pi = \sqrt{ep}$ and $e = \pm 1$. Let $K_P := \mathbb{Q}_P(\sqrt{ep})$. We show $(\Pi, \bar{x})_P = (p, \bar{x})_p$ for every $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^*$. Suppose $(p, \bar{x})_p = 1$. Then $\bar{x} \in \mathbb{Z}_p^{*2}$. So $\bar{x} \in (O_{K_P}^*)^2$. Thus $(\Pi, \bar{x})_P = 1$. Suppose $\bar{x} \in (O_{K_P}^*)^2$ but not in $(\mathbb{Z}_p^*)^2$. Then $[\mathbb{Q}_P(\sqrt{\bar{x}}\,) : \mathbb{Q}_p] = 2$ since $\bar{x} \notin (\mathbb{Z}_p^*)^2$. On the other hand,

$$\sqrt{\bar{x}} \in O_{K_P}^* \subseteq \mathbb{Q}_P(\sqrt{ep}).$$

So $\mathbb{Q}_P(\sqrt{\bar{x}}\,) \subseteq \mathbb{Q}_P(\sqrt{ep})$. So

$$[\mathbb{Q}_P(\sqrt{ep}) : \mathbb{Q}_p] = [\mathbb{Q}_P(\sqrt{ep}) : \mathbb{Q}_P(\sqrt{\bar{x}}\,)] \cdot [\mathbb{Q}_P(\sqrt{\bar{x}}\,) : \mathbb{Q}_p]$$

So we get $2 = [\mathbb{Q}_P(\sqrt{ep}) : \mathbb{Q}_P(\sqrt{\bar{x}}\,)] \cdot 2$. Therefore $\mathbb{Q}_P(\sqrt{ep}\,) = \mathbb{Q}_P(\sqrt{\bar{x}}\,)$. This implies $\bar{x} = ep\,t^2$ for some $t \in \mathbb{Q}_p$. This contradicts that $\bar{x}$ is a unit. So $\bar{x} \in (O_{K_P}^*)^2$ implies $\bar{x} \in (\mathbb{Z}_p^*)^2$ meaning $(\Pi, \bar{x})_P = 1 \Longrightarrow (p, \bar{x})_p = 1$.

3.2 Local Root Numbers in Quadratic Fields

In this section we find some local root numbers in quadratic fields. Throughout this section n is a positive square free integer and $e = \pm 1$ in a quadratic number field $\mathbb{Q}(\sqrt{en}\,)$.

Lemma 3.4. *Let $K := \mathbb{Q}(\sqrt{en}\,)$ be a quadratic number field. Suppose an odd rational prime p is split in K, meaning $p\,O_K = PP'$, where P and P' are prime ideals in O_K. Then $r_P(\epsilon) = 1$, where ϵ is a non-square unit in K_P^*.*

Proof. The inertia degree $f(P|p)$ and the ramification index $e(P|p)$ are all 1. So $[K_P : \mathbb{Q}_p] = 1$ and $r_P(x) = r_p(x)$ for any $x \in K_P^*$. Write $K_P^*/K_P^{*2} = \{1, \epsilon, p, \epsilon p\}$. Define a quadratic character $\alpha : K_P^* \longrightarrow \{1, -1\}$ by $\alpha(x) = (\epsilon, x)_P$. Then by Proposition 2.6, $\alpha(U_{K_P}) = 1$. So the conductor $f_\epsilon = O_{K_P}$. This implies $\mathcal{N} f_\epsilon = 1$. It is clear that the local absolute different $D_{K_P} = (1)$ since p is unramified (see p. 62 in [12]). Thus $f_\epsilon D_{K_P} = (1)$. By Theorem 2.13

$$\begin{aligned} r_p(\epsilon) &= \frac{1}{\sqrt{\mathcal{N} f_\epsilon}} \sum_{x \in U_{K_P} \bmod^* f_\epsilon} \alpha(x)\psi_{K_P}(x) \\ &= \frac{1}{\sqrt{1}} \sum_{x=1} \alpha(x)\psi_{K_P}(x) \\ &= (\epsilon, 1)_p = 1. \end{aligned}$$

Therefore $r_P(\epsilon) = 1$. □

Lemma 3.5. *Suppose $K := \mathbb{Q}(\sqrt{en})$ be a quadratic field. Let p be a rational odd prime which is split in K meaning $pO_K = PP'$, where P and P' are prime ideals in O_{K_P}. Then $r_P(p) = 1$ if $p \equiv 1 \pmod 4$ and $r_P(p) = -i$ if $p \equiv 3 \pmod 4$.*

Proof. The local root numbers $r_P(x)$ and $r_p(x)$ are the same since $[K_P : \mathbb{Q}_p] = e(P|p)f(P|p) = 1$. Define a quadratic character $\alpha : K_P^* \longrightarrow \{\pm 1\}$ by $\alpha(x) = (p, x)_p$. Then $f_p = P$ since $\alpha(1+P) = 1$ by Theorem 1.8. The prime P is unramified in K. So $D_{K_P} = (1)$. Thus $f_p D_{K_P} = P = (p)$. By Theorem 2.13

$$\begin{aligned} r_P(p) &= \frac{1}{\sqrt{\mathcal{N} f_p}} \sum_{x \in U_{K_P} \ mod^* \ f_p} \alpha(px)\psi_{K_P}(p^{-1}x) \\ &= \frac{1}{\sqrt{p}} \cdot (p, p)_p \cdot \sum_{x \in U_{K_P} \ mod^* \ P} \alpha(x)\psi_{K_P}(\frac{x}{p}) \\ &= \frac{1}{\sqrt{p}} \cdot (p, -1)_p \cdot \sum_{j \in \mathbb{F}_p^*} \alpha(j) e^{\frac{2\pi j i}{p}}. \end{aligned}$$

(1) If $p \equiv 1 \pmod 4$, then by Lemma 3.3

$$r_P(p) = \frac{1}{\sqrt{p}} \cdot 1 \cdot (\frac{1}{p}) \cdot \sqrt{p} = 1.$$

(2) If $p \equiv 3 \pmod 4$, then by Lemma 3.3

$$r_P(p) = \frac{1}{\sqrt{p}} \cdot (-1) \cdot (\frac{1}{p}) \cdot i \cdot \sqrt{p} = -i.$$

□

Lemma 3.6. *Suppose $K := \mathbb{Q}(\sqrt{en})$ be a quadratic field. Let p be a rational odd prime which is inert in K meaning $pO_K = P$, where P is a prime ideal in O_K. Then $r_P(\epsilon) = 1$, where ϵ is a non-square unit in K_P.*

Proof. Write $K_P^*/K_P^{*2} = \{1, \epsilon, p, \epsilon p\}$, where ϵ is a non-square unit in K_P. Suppose $\alpha : K_P^* \longrightarrow \{1, -1\}$ is a map defined by $\alpha(x) = (\epsilon, x)_P$. Then $\alpha(U_{K_P}) = 1$. So by the definition of a conductor, $f_\epsilon = (1)$. This implies $\mathcal{N} f_\epsilon = 1$. The local

absolute different $D_{K_P} = O_{K_P}$ since p is unramified in K_P (see p. 62 in [12]). Thus $f_\epsilon D_{K_P} = (1)$. So by Theorem 2.13

$$\begin{aligned} r_P(\epsilon) &= \frac{1}{\sqrt{\mathcal{N} f_\epsilon}} \sum_{x \in U_{K_P} \ mod^* \ f_\epsilon} \bar{\alpha}(x)\psi_{K_P}(x) \\ &= \sum_{x=1} \alpha(x)\psi_{K_P}(x) \\ &= (\epsilon, 1)_P \ = \ 1 \end{aligned}$$

□

Lemma 3.7. *Suppose $K := \mathbb{Q}(\sqrt{en})$ be a quadratic field. Let p be a rational odd prime which is inert in K meaning $pO_K = P$, where P is a prime ideal in O_K. Then $r_P(p) = -1$.*

Proof. Define a quadratic character $\alpha : K_P^* \longrightarrow \{1, -1\}$ by $\alpha(x) = (p, x)_P$. It is clear that α is not unramified since $\alpha(\epsilon) = -1$, where ϵ is a non-square in K_P^*. Let $u \in 1 + P$. We show $u \in (\overline{K_P}^*)^2$. Consider a polynomial $f(x) := x^2 - u$ in $O_K[x]$. Then

$$f(x) \ \equiv \ x^2 - 1 \pmod{P}.$$

So we have two different zeros 1 and -1 of $f(x)$ in $\overline{K_P}^*$ since p is odd. This means the polynomials $x - 1$ and $x + 1$ are relatively prime in $\overline{K_P}[x]$. Thus by Hensel's Lemma,

$$\begin{aligned} x^2 - u &= (x - a)(x - b) \quad \text{in} \quad O_{K_P}[x] \\ &= x^2 - (a + b)x + ab \end{aligned}$$

This implies $u = -ab = b^2$ in O_{K_P}. So $u \in O_{K_P}^{*2}$. Therefore $\alpha(1 + P) = 1$. So the conductor $f_p = P$ and $\mathcal{N} f_p = p^{f(P|p)} = p^2$. The local absolute different $D_{K_P} = O_{K_P}$ since P is unramified (see p. 62 in [12]). Thus

$$f_p D_{K_P} = P = (p).$$

So by Theorem 2.13,

$$\begin{aligned} r_P(p) &= \frac{1}{\sqrt{\mathcal{N}f_p}} \sum_{x \in U_{K_P} \bmod^* f_p} \alpha(p^{-1}x)\psi_{K_P}(p^{-1}x) \\ &= \frac{1}{p} \sum_{x \in U_{K_P} \bmod^* f_p} \alpha(px)\psi_{K_P}(p^{-1}x) \\ &= \frac{1}{p} \cdot (p,p)_P \cdot \sum_{x \in U_{K_P} \bmod^* f_p} \alpha(x)\psi_{K_P}(p^{-1}x) \\ &= \frac{1}{p} \cdot (p,-1)_p \cdot \{ \sum_{x \in \mathbb{F}_{p^2}^*, \mathrm{Tr}(x)=0} \alpha(x) + \sum_{j=1}^{p-1} (\sum_{x \in \mathbb{F}_{p^2}^*, \mathrm{Tr}(x)=j} \alpha(x)) e^{\frac{2\pi j i}{p}} \} \end{aligned}$$

(1) If $p \equiv 1 \pmod 4$, then

$$\begin{aligned} r_P(p) &= \frac{1}{p} \cdot (p,-1)_p \cdot \{ \sum_{x \in \mathbb{F}_{p^2}^*, \mathrm{Tr}(x)=0} \alpha(x) + \sum_{j=1}^{p-1} (\sum_{x \in \mathbb{F}_{p^2}^*, \mathrm{Tr}(x)=j} \alpha(x)) e^{\frac{2\pi j i}{p}} \} \\ &= \frac{1}{p} \cdot 1 \cdot \{ -(p-1) + \sum_{j=1}^{p-1} e^{\frac{2\pi j i}{p}} \} \quad \text{by Lemma 3.2} \\ &= \frac{1}{p} \cdot \{ -(p-1) + (-1) \} = -1. \end{aligned}$$

(2) If $p \equiv 3 \pmod 4$, then

$$\begin{aligned} r_P(p) &= \frac{1}{p} \cdot (p,-1)_p \cdot \{ \sum_{x \in \mathbb{F}_{p^2}^*, \mathrm{Tr}(x)=0} \alpha(x) + \sum_{j=1}^{p-1} (\sum_{x \in \mathbb{F}_{p^2}^*, \mathrm{Tr}(x)=j} \alpha(x)) e^{\frac{2\pi j i}{p}} \} \\ &= \frac{1}{p} \cdot (-1) \cdot \{ (p-1) - \sum_{j=1}^{p-1} e^{\frac{2\pi j i}{p}} \} \quad \text{by Lemma 3.2} \\ &= \frac{1}{p} \cdot (-1) \cdot \{ (p-1) - (-1) \} \ = \ -1. \end{aligned}$$

□

Lemma 3.8. *Suppose $K := \mathbb{Q}(\sqrt{en})$ be a quadratic field. Then $r_P(\epsilon) = -1$ for every non-dyadic ramified prime P in K, where ϵ is a non-square unit in K_P^*.*

Proof. First we define a quadratic character $\alpha(x) := (\epsilon, x)_P$ on K_P^* where $(\epsilon, x)_P$ is the Hilbert symbol on K_P^*. Then $\alpha(U_{K_P}) = 1$ by Proposition 2.6. So $f_\epsilon = O_{K_P}$.

So $\mathcal{N}f_\epsilon = 1$. The absolute different $D_{K_P} = \Pi O_{K_P}$ is clear, where $\Pi = \sqrt{en}$. So by the formula in Theorem 2.13,

$$\begin{aligned} r_P(\epsilon) &= \frac{1}{\sqrt{\mathcal{N}f_\epsilon}} \sum_{x \in U_{K_P} \ mod^* \ f_\epsilon} \alpha(\Pi^{-1}x)\psi_{K_P}(\Pi^{-1}x) \\ &= \frac{1}{\sqrt{1}} \sum_{x=1} \alpha(\Pi^{-1}x)\psi_{K_P}(\Pi^{-1}x) \\ &= \alpha(\Pi) \cdot \psi_{K_P}(\frac{1}{\Pi}) \\ &= (\epsilon, \Pi)_P = -1 \qquad \text{since } \psi_{K_P}(\frac{1}{\Pi}) = 1 \text{ and by Proposition 2.6.} \end{aligned}$$

□

3.3 Different Arf Equivalence Classes in Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{ep_1 \cdots p_n}\ )$, where $p_1, \cdots, p_n$ are distinct rational primes, $p_j \equiv 3 \pmod 4$ for each j and $e = \pm 1$.

(1) Suppose an odd rational prime p is split in K. That is, $p\,O_K = PP'$ for prime ideals P and P' in O_K. Then $[K_P : \mathbb{Q}_p] = 1$. Write $K_P^*/K_P^{*2} = \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{1, \epsilon, p, \epsilon p\}$, where ϵ is a non-square unit in $\mathbb{Q}_p$. Note that $r_P(a) = r_p(a)$ for every $a \in K_P^*/K_P^{*2}$ since $[K_P : \mathbb{Q}_p] = 1$. It is clear that $r_p(1) = 1$. By Theorem 2.14 and Lemma 3.4

$$r_p(\epsilon p) = (\epsilon, p)_p \cdot r_p(\epsilon) \cdot r_p(p) = (-1) \cdot 1 \cdot r_p(p) = -r_p(p).$$

Thus by Lemma 3.5,

$$r_p(\epsilon p) = \begin{cases} -1 & \text{if } p \equiv 1 \pmod 4 \\ i & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{3.26}$$

(2) Suppose p is inert in K. Let $p\,O_K = P$, where P is a prime ideal in O_K. Write $K_P^*/K_P^{*2} = \{1, \epsilon, p, \epsilon p\}$, where ϵ is a non-square unit in K_P. Then by Theorem 2.14,

Lemma 3.6 and Lemma 3.7,

$$\begin{aligned} r_P(\epsilon p) &= (\epsilon, p)_P \cdot r_P(\epsilon) \cdot r_P(p) \\ &= (-1) \cdot 1 \cdot (-1) = 1. \end{aligned}$$

Theorem 3.9. *Suppose $K := \mathbb{Q}(\sqrt{en})$ be a quadratic field, where $e = \pm 1$ and n is a square free positive integer. Let P be a non-dyadic split prime or a non-dyadic inert prime in K, where $P \cap \mathbb{Z} = (p) \neq (2)$. Then $Arf(r_P) = 1$.*

Proof. (1) Suppose P is split in K. Write $K_P^*/K_P^{*2} = \{1, \epsilon, p, \epsilon p\}$.

(1a) If $p \equiv 1 \pmod 4$, then by Lemma 3.4 and Lemma 3.5,

$$r_P(a) = \begin{cases} 1 & \text{if } a = 1 \\ 1 & \text{if } a = \epsilon \\ 1 & \text{if } a = p \\ -1 & \text{if } a = \epsilon p. \end{cases} \tag{3.27}$$

Therefore

$$\begin{aligned} \mathrm{Arf}(r_P) &= \frac{1}{2} \sum_{a \in K_P^*/K_P^{*2}} r_P(a) \\ &= \frac{1}{2}\{r_p(1) + r_p(\epsilon) + r_p(p) + r_p(\epsilon p)\} \\ &= \frac{1}{2}\{1 + 1 + 1 + (-1)\} = 1. \end{aligned}$$

(1b) If $p \equiv 3 \pmod 4$, then by Lemma 3.4 and Lemma 3.5,

$$r_P(a) = \begin{cases} 1 & \text{if } a = 1 \\ 1 & \text{if } a = \epsilon \\ -i & \text{if } a = p \\ i & \text{if } a = \epsilon p. \end{cases} \tag{3.28}$$

Therefore

$$\begin{aligned}\mathrm{Arf}(r_P) &= \frac{1}{2}\sum_{a\in K_P^*/K_P^{*2}} r_P(a)\\ &= \frac{1}{2}\{r_p(1)+r_p(\epsilon)+r_p(p)+r_p(\epsilon p)\}\\ &= \frac{1}{2}\{1+1+(-i)+i\}=1.\end{aligned}$$

(2) Suppose P is an inert prime in K. Then $P=(p)$. Write $K_P^*/K_P^{*2}=\{1,\epsilon,p,\epsilon p\}$. Then by Lemma 3.6 and Lemma 3.7,

$$r_P(a) = \begin{cases} 1 & \text{if } a=1\\ 1 & \text{if } a=\epsilon\\ -1 & \text{if } a=p\\ 1 & \text{if } a=\epsilon p.\end{cases} \tag{3.29}$$

Therefore

$$\begin{aligned}\mathrm{Arf}(r_P) &= \frac{1}{2}\sum_{a\in K_P^*/K_P^{*2}} r_P(a)\\ &= \frac{1}{2}\{r_P(1)+r_P(\epsilon)+r_P(p)+r_P(\epsilon p)\}\\ &= \frac{1}{2}\{1+1+(-1)+1\}=1.\end{aligned}$$

□

Theorem 3.10. *Suppose $K:=\mathbb{Q}(\sqrt{en}\,)$ be a quadratic field, where $e=\pm 1$ and n is a square-free positive integer. Let P be a non-dyadic ramified prime in K with $P\bigcap\mathbb{Z}=(p)$, where p is a positive rational prime and is congruent to 3 modulo 4. Then $Arf(r_P)=i$ or $-i$.*

Proof. By Theorem 1.29 p must divide n and $pO_K=P^2$. Let $\Pi=\sqrt{en}$. Write $K_P^*/K_P^{*2}=\{1,\epsilon,\Pi,\epsilon\Pi\}$. Define a map $\alpha: K_P^*\longrightarrow\{1,-1\}$ by $\alpha(x)=(\Pi,x)_P$. Then $\alpha(1+P)=1$ by Theorem 1.8. So $f_\Pi=P$. Thus $\mathcal{N}f_\Pi=p$. The local

absolute different $D_{K_P} = \Pi O_{K_P}$ is clear. So

$$\begin{aligned} f_\Pi D_{K_P} &= \Pi P O_{K_P} = \Pi(p, \Pi) \\ &= p(\Pi, \frac{\Pi^2}{p}) = pO_{K_P} \end{aligned}$$

since $\frac{\Pi^2}{p} \in \mathbb{Z}$ is a unit in $\mathbb{Z}_p$. By Theorem 2.13

$$\begin{aligned} r_P(\Pi) &= \frac{1}{\sqrt{p}} \sum_{x \in U_{K_P} \bmod^* f_\Pi} \bar{\alpha}(p^{-1}x)\psi_{K_P}(p^{-1}x) \\ &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot \sum_{x \in U_{K_P} \bmod^* P} \alpha(px)\psi_{K_P}(p^{-1}x) \\ &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot \sum_{x \in \mathbb{F}_p^*} (\frac{x}{p}) e^{\frac{4\pi x i}{p}} \\ &= i \cdot (\Pi, p)_P \cdot (\frac{2}{p}) \end{aligned}$$

So we get $r_P(\Pi) = i$ or $-i$. By the way,

$$r_P(\epsilon\Pi) = (\epsilon, \Pi)_P \cdot r_P(\epsilon) \cdot r_P(\Pi) = (-1) \cdot (-1) \cdot r_P = r_P(\Pi)$$

by Lemma 3.8. So

$$\begin{aligned} \mathrm{Arf}(r_P) &= \frac{1}{2} \sum_{a \in K_P^*/K_P^{*2}} r_P(a) \\ &= \frac{1}{2}\{r_P(1) + r_P(\epsilon) + r_P(\Pi) + r_P(\epsilon\Pi)\} \\ &= \frac{1}{2}\{1 + (-1) + r_P(\Pi) + r_P(\epsilon\Pi)\} = r_P(\Pi) = e_{K_P} \cdot i, \text{ where } e_{K_P} = \pm 1. \end{aligned}$$

□

Theorem 3.11. *There are infinitely many classes of quadratic number fields up to Arf equivalence.*

Proof. It is enough to show that two number fields $K := \mathbb{Q}(\sqrt{p_1 \cdots p_n})$ and $L := \mathbb{Q}(\sqrt{q_1 \cdots q_m})$ are not Arf equivalent when $n \neq m$, where $p_1, \cdots, p_n$ and $q_1, \cdots, q_m$ are pairwise distinct rational primes respectively and $p_k, q_l \equiv 3 \pmod 4$ for each

k and l. Suppose p and q are odd rational primes which are ramified in K and L respectively, i.e., $p\,O_K = P^2$ and $q\,O_L = Q^2$ for prime ideals P in O_K and Q in O_L. It is known $p \in \{p_i | \, i = 1, \cdots, n\}$ and $q \in \{q_j | \, j = 1, \cdots, m\}$ by Theorem 1.29. So there are exactly n non-dyadic ramified primes in K and m non-dyadic ramified primes in L. Write $K_P^*/K_P^{*2} = \{1, \epsilon_K, \Pi_K, \epsilon_K \Pi_K\}$ and write $L_Q^*/L_Q^{*2} = \{1, \epsilon_L, \Pi_L, \epsilon_L \Pi_L\}$, where ϵ_K and ϵ_L are non-square units in K_P and L_Q respectively and $\Pi_K = \sqrt{p_1 \cdots p_n}$ and $\Pi_L = \sqrt{q_1 \cdots q_m}$. Then by Theorem 3.10, $\mathrm{Arf}(r_P) = e_K i$ and $\mathrm{Arf}(r_Q) = e_L i$, where $e_K, e_L \in \{1, -1\}$. On the other hand, there is no finite non-dyadic unramified prime with an Arf invariant i or $-i$ by Theorem 3.9. In order for K and L to be Arf equivalent any dyadic prime (any non-dyadic prime respectively) P in O_K can not be matched with a non-dyadic prime (a dyadic prime respectively) Q in O_L since $|K_P^*/K_P^{*2}| \neq |L_Q^*/L_Q^{*2}|$. This means there should be a one-to-one correspondence between non-dyadic ramified primes in K and non-dyadic ramified primes in L, and this is impossible since $n \neq m$. Therefore K and L are not Arf equivalent. □

Even though there are infinitely many Arf equivalence classes of quadratic fields, we can classify some quadratic fields into finite classes. Let $\mathcal{K}$ be the set of all quadratic fields of the form $\mathbb{Q}(\sqrt{ep})$, where $e = \pm 1$ and p is a rational positive prime. We will see that $K = \mathbb{Q}(\sqrt{ep})$ and $L = \mathbb{Q}(\sqrt{e'p'})$ in $\mathcal{K}$ are Arf equivalent if and only if $e = e'$ and $p = p' \pmod 8$. The manuscript of Conner-Yui tells how to compute root numbers in some cases (see Corollary 2.11 of this thesis or [5]). In this section we will compute them using Tate's formula.

Lemma 3.12. *Suppose $K := \mathbb{Q}(\sqrt{ep})$, where p is an odd positive rational prime in $\mathbb{Q}$ with $p\,O_K = P^2$ for a prime ideal P in O_K and $e = \pm 1$. Let $\Pi = \sqrt{ep}$. Then*

$$r_P(\Pi) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \\ -ei & \text{if } p \equiv 3 \pmod 8 \\ -1 & \text{if } p \equiv 5 \pmod 8 \\ ei & \text{if } p \equiv 7 \pmod 8. \end{cases} \tag{3.30}$$

Proof. Write $K_P^*/K_P^{*2} = \{1, \epsilon, \Pi, \epsilon\Pi\}$. We first find the conductor f_Π. For a quadratic character $\alpha : K_P^* \longrightarrow \{1, -1\}$ defined by $\alpha(x) = (\Pi, x)_P$, $\alpha(1+P) = 1$ by Theorem 1.8. So $f_\Pi = P$. So $\mathcal{N}f_\Pi = p^{f(P|p)} = p$. The local absolute different $D_{K_P} = \Pi O_{K_P}$ since $D_{K_P} = f'(\Pi)O_{K_P} = 2\Pi O_{K_P} = \Pi O_{K_P}$ and $2 \in O_{K_P}$, where $f(x) = irr(\Pi, O_{K_P})$. So

$$f_\Pi D_{K_P} = \Pi(p, \Pi) = (p\Pi, ep) = p(\Pi, e) = p\, O_{K_P}.$$

On the other hand,

$$U_{K_P}/(1+P) \;\cong\; \overline{K_P} \;\cong\; \mathbb{F}_p^*,$$

where $\overline{K_P}$ is the residue class field of K_P. So by the formula (1) of Theorem 2.13,

$$\begin{aligned} r_P(\Pi) &= \frac{1}{\sqrt{\mathcal{N}f_\Pi}} \sum_{x \in U_{K_P} \; mod^* \; f_\Pi} \alpha(p^{-1}x) \cdot \psi_{K_P}(p^{-1}x) \\ &= \frac{1}{\sqrt{p}} \sum_{x \in U_{K_P} \; mod^* \; f_\Pi} \alpha(px) \cdot \psi_{K_P}(\frac{x}{p}) \\ &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot \sum_{x \in \mathbb{F}_p^*} (\Pi, x)_P \; e^{\frac{4\pi x i}{p}} \\ &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot \sum_{x \in \mathbb{F}_p^*} (p, x)_p \; e^{\frac{4\pi x i}{p}} \\ &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot \sum_{x=1}^{p-1} (\frac{x}{p}) \; e^{\frac{4\pi x i}{p}} \end{aligned}$$

by the argument of the last part of the section 3.1.

If $p \equiv 1 \pmod 8$ and $K_P = \mathbb{Q}_P(\sqrt{p}\,)$, then by Lemma 3.3,

$$\begin{aligned} r_P(\Pi) &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot \sqrt{p}\ \cdot (\frac{2}{p}) \\ &= (\Pi, p)_P \cdot (\frac{2}{p}) = 1 \end{aligned}$$

since $(\Pi, p)_P = (\Pi, (\sqrt{p}\,)^2)_P = 1$ and $(\frac{2}{p}) = 1$.

If $p \equiv 1 \pmod 8$ and $K_P = \mathbb{Q}_P(\sqrt{-p}\,)$, then by Lemma 3.3,

$$\begin{aligned} r_P(\Pi) &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot \sqrt{p}\ \cdot (\frac{2}{p}) \\ &= (\Pi, p)_P \cdot (\frac{2}{p}) = 1 \end{aligned}$$

since $(\Pi, p)_P = (\Pi, -(\sqrt{-p}\,)^2)_P = (\Pi, -1)_P = (p, -1)_p = 1$ and $(\frac{2}{p}) = 1$.

If $p \equiv 3 \pmod 8$ and $K_P = \mathbb{Q}_P(\sqrt{p}\,)$, then by Lemma 3.3,

$$\begin{aligned} r_P(\Pi) &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot i \cdot \sqrt{p}\ \cdot (\frac{2}{p}) \\ &= i \cdot (\Pi, p)_P \cdot (\frac{2}{p}) = -i \end{aligned}$$

since $(\Pi, p)_P = (\Pi, (\sqrt{p}\,)^2)_P = 1$ and $(\frac{2}{p}) = -1$.

If $p \equiv 3 \pmod 8$ and $K_P = \mathbb{Q}_P(\sqrt{-p}\,)$, then by Lemma 3.3,

$$\begin{aligned} r_P(\Pi) &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot i \cdot \sqrt{p}\ \cdot (\frac{2}{p}) \\ &= i \cdot (\Pi, p)_P \cdot (\frac{2}{p}) = i \end{aligned}$$

since $(\Pi, p)_P = (\Pi, -(\sqrt{-p}\,)^2)_P = (\Pi, -1)_P = (p, -1)_p = -1$ and $(\frac{2}{p}) = -1$.

If $p \equiv 5 \pmod 8$ and $K_P = \mathbb{Q}_P(\sqrt{p}\,)$, then by Lemma 3.3,

$$\begin{aligned} r_P(\Pi) &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot \sqrt{p}\ \cdot (\frac{2}{p}) \\ &= (\Pi, p)_P \cdot (\frac{2}{p}) = -1 \end{aligned}$$

since $(\Pi, p)_P = (\Pi, (\sqrt{p}\,)^2)_P = 1$ and $(\frac{2}{p}) = -1$.

If $p \equiv 5 \pmod 8$ and $K_P = \mathbb{Q}_P(\sqrt{-p}\,)$, then by Lemma 3.3,

$$\begin{aligned} r_P(\Pi) &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot \sqrt{p}\ \cdot (\frac{2}{p}) \\ &= (\Pi, p)_P \cdot (\frac{2}{p}) = -1 \end{aligned}$$

since $(\Pi, p)_P = (\Pi, -(\sqrt{-p}\,)^2)_P = (\Pi, -1)_P = (p, -1)_p = 1$ and $(\frac{2}{p}) = -1$.

If $p \equiv 7 \pmod 8$ and $K_P = \mathbb{Q}_P(\sqrt{p}\,)$, then by Lemma 3.3,

$$\begin{aligned} r_P(\Pi) &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot i \cdot \sqrt{p}\ \cdot (\frac{2}{p}) \\ &= i \cdot (\Pi, p)_P \cdot (\frac{2}{p}) = i \end{aligned}$$

since $(\Pi, p)_P = (\Pi, (\sqrt{p}\,)^2)_P = 1$ and $(\frac{2}{p}) = 1$.

If $p \equiv 7 \pmod 8$ and $K_P = \mathbb{Q}_P(\sqrt{-p}\,)$, then by Lemma 3.3,

$$\begin{aligned} r_P(\Pi) &= \frac{1}{\sqrt{p}} \cdot (\Pi, p)_P \cdot i \cdot \sqrt{p}\ \cdot (\frac{2}{p}) \\ &= i \cdot (\Pi, p)_P \cdot (\frac{2}{p}) = -i \end{aligned}$$

since $(\Pi, p)_P = (\Pi, -(\sqrt{-p}\,)^2)_P = (\Pi, -1)_P = (p, -1)_p = -1$ and $(\frac{2}{p}) = 1$.

□

Lemma 3.13. *Suppose $K := \mathbb{Q}(\sqrt{ep}\,)$ be a quadratic field, where $e = \pm 1$ and p is a rational positive odd prime. Let P be a ramified prime in O_K with $P \bigcap \mathbb{Z} = (p)$. Then*

$$Arf(r_P) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \\ -ei & \text{if } p \equiv 3 \pmod 8 \\ -1 & \text{if } p \equiv 5 \pmod 8 \\ ei & \text{if } p \equiv 7 \pmod 8. \end{cases} \tag{3.31}$$

Proof. Write $K_P^*/K_P^{*2} = \{1, \epsilon, \Pi, \epsilon\Pi\}$, where ϵ is a non-square unit in K_P and Π is a prime element in K_P. Then by Proposition 2.6, Theorem 2.14 and Lemma 3.8

$$r_P(\epsilon\Pi) = (\epsilon, \Pi)_P \cdot r_P(\epsilon) \cdot r_P(\Pi) = (-1) \cdot (-1) \cdot r_P(\Pi) = r_P(\Pi).$$

Therefore

$$\begin{aligned} \mathrm{Arf}(r_P) &= \frac{1}{2} \sum_{x \in K_P^*/K_P^{*2}} r_P(x) \\ &= \frac{1}{2}\{r_P(1) + r_P(\epsilon) + r_P(\Pi) + r_P(\epsilon\Pi)\} \\ &= \frac{1}{2}\{1 + (-1) + r_P(\Pi) + r_P(\Pi)\} = r_P(\Pi). \end{aligned}$$

Then Lemma 3.13 follows from Lemma 3.12. □

Recall that $\mathcal{K}$ is the set of all quadratic number fields of the form $\mathbb{Q}(\sqrt{ep}\,)$, where $e = \pm 1$ and p is a positive rational prime.

Theorem 3.14. *There are ten Arf equivalence classes of quadratic number fields $\mathcal{K}$. They are represented by $\mathbb{Q}(\sqrt{d}\,)$ for $d = \pm 2, \pm 3, \pm 5, \pm 7, \pm 17$. The quadratic number field $\mathbb{Q}(\sqrt{n}\,)$, where $|n|$ is a prime, is Arf equivalent to $\mathbb{Q}(\sqrt{d}\,)$ with d determined as follows:*

$$d = \begin{cases} sign(n) \cdot 2 & \text{if} \quad |n| \equiv 2 \pmod 8 \\ sign(n) \cdot 3 & \text{if} \quad |n| \equiv 3 \pmod 8 \\ sign(n) \cdot 5 & \text{if} \quad |n| \equiv 5 \pmod 8 \\ sign(n) \cdot 7 & \text{if} \quad |n| \equiv 7 \pmod 8 \\ sign(n) \cdot 17 & \text{if} \quad |n| \equiv 1 \pmod 8. \end{cases} \tag{3.32}$$

Proof. First we show that ten representatives are pairwise distinct up to Arf equivalence. It is enough to show that any two number fields in each of the following sets $\{\mathbb{Q}(\sqrt{2}\,), \mathbb{Q}(\sqrt{3}\,), \mathbb{Q}(\sqrt{5}\,)\}$ and $\{\mathbb{Q}(\sqrt{-2}\,), \mathbb{Q}(\sqrt{-3}\,), \mathbb{Q}(\sqrt{-5}\,)\}$ are not Arf equivalent by Theorem 1.22 and Theorem 2.28. There is no non-dyadic ramified prime

in $\mathbb{Q}(\sqrt{2}\,)$ and $\mathbb{Q}(\sqrt{-2}\,)$. This implies that there is no non-dyadic prime with Arf invariant $\pm i$ or -1 in $\mathbb{Q}(\sqrt{2}\,)$ and $\mathbb{Q}(\sqrt{-2}\,)$ by Theorem 3.9. So $\mathbb{Q}(\sqrt{2}\,)$ ($\mathbb{Q}(\sqrt{-2}\,)$ respectively) is not Arf equivalent to $\mathbb{Q}(\sqrt{3}\,)$ and $\mathbb{Q}(\sqrt{5}\,)$ ($\mathbb{Q}(\sqrt{-3}\,)$ and $\mathbb{Q}(\sqrt{-5}\,)$ respectively). Now we show $\mathbb{Q}(\sqrt{3}\,)$ and $\mathbb{Q}(\sqrt{5}\,)$ are not Arf equivalent. There is no finite non-dyadic prime with Arf invariant $-i$ in $\mathbb{Q}(\sqrt{5}\,)$ by Theorem 3.9 and Lemma 3.13. On the other hand, we have a non-dyadic ramified prime with Arf invariant $-i$ in $\mathbb{Q}(\sqrt{3}\,)$ by Lemma 3.13. So $\mathbb{Q}(\sqrt{3}\,)$ and $\mathbb{Q}(\sqrt{5}\,)$ are not Arf equivalent. By the similar argument $\mathbb{Q}(\sqrt{-3}\,)$ and $\mathbb{Q}(\sqrt{-5}\,)$ are not Arf equivalent. So it is proved that ten representatives are all pairwise distinct up to Arf equivalence. Suppose two quadratic number fields $K := \mathbb{Q}(\sqrt{ep}\,)$ and $L := \mathbb{Q}(\sqrt{eq}\,)$ are given, where $e = \pm 1$ and p and q are odd and $p \equiv q \pmod 8$. It is clear that -1 is not a square in K since -1 and ep are not in the same square class in $\mathbb{Q}$. By the same argument $-1 \notin L^{*2}$. By the Tschebotarev density theorem (see p. 169, [12]), there are infinitely many primes P and P' in K (Q and Q' in L respectively) such that $[K(\sqrt{-1}\,)_P : K_P] = 1$ and $[K(\sqrt{-1}\,)_{P'} : K_{P'}] = 2$ ($[L(\sqrt{-1}\,)_Q : L_Q] = 1$ and $[L(\sqrt{-1}\,)_{Q'} : L_{Q'}] = 2$ respectively). This means there are infinitely many type I spaces and type II spaces occurring among the K_P and L_Q. So we have a one to one correspondence

$$\begin{array}{c} \{\text{non-dyadic split or non-dyadic inert places in } K\} \\ \Big\downarrow{\scriptstyle T_1} \\ \{\text{non-dyadic split or non-dyadic inert places in } L\} \end{array} \tag{3.33}$$

satisfying $\mathrm{Arf}(r_P) = \mathrm{Arf}(r_{T_1 P})$, $\mathrm{type}[(\ ,\ )_P] = \mathrm{type}[(\ ,\ )_{T_1 P}]$, and $|K_P^*/K_P^{*2}| = |L_{T_1 P}^*/L_{T_1 P}^{*2}|$ by Theorem 3.9.

Suppose P and Q are non-dyadic ramified primes in K and L respectively. Then $P \bigcap \mathbb{Z} = (p)$ and $Q \bigcap \mathbb{Z} = (q)$. Recall $p \equiv q \pmod 8$. Let's examine the case $p \equiv 1 \pmod 4$. Then $q \equiv 1 \pmod 4$. So -1 is a square in K_P and L_Q since -1 is a square

in $\mathbb{Q}_p$ and $\mathbb{Q}_q$ respectively. Next, examine the case $p \equiv 3 \pmod 4$. Then $q \equiv 3 \pmod 4$. So -1 is not a square in $\mathbb{Q}_p$ and $\mathbb{Q}_q$. Thus -1 is also not a square in K_P and L_Q. The reason is as follows. Assume -1 is a square in K_P. Then $\sqrt{-1} \in K_P$. So

$$2 = [K_P : \mathbb{Q}_p] = [K_P : \mathbb{Q}_p(\sqrt{-1}\,)] \cdot [\mathbb{Q}_p(\sqrt{-1}\,) : \mathbb{Q}_p].$$

Thus $K_P = \mathbb{Q}_p(\sqrt{-1}\,)$ since $[\mathbb{Q}_p(\sqrt{-1}\,) : \mathbb{Q}_p] = 2$. This means -1 and ep are in the same local square classes in $\mathbb{Q}_p$. It is impossible since $\frac{ep}{-1} \notin \mathbb{Q}_p^{*2}$. By similar argument -1 is not a square in L_Q. So we have a one to one correspondence

$$\{\text{non-dyadic ramified place in } K\} \xrightarrow{T_2} \{\text{non-dyadic ramified place in } L\}$$

satisfying $\mathrm{Arf}(r_P) = \mathrm{Arf}(r_{T_2P})$, $\mathrm{type}[(\ ,\ )_P] = \mathrm{type}[(\ ,\ )_{T_2P}]$, and $|K_P^*/K_P^{*2}| = |L_{T_2P}^*/L_{T_2P}^{*2}|$ by Lemma 3.13. Suppose we have a dyadic prime P in K and a dyadic prime Q in L. If $p \equiv 1 \pmod 8$, then P and Q are split. This means $[K_P : \mathbb{Q}_2] = 1$ and $[L_Q : \mathbb{Q}_2] = 1$. So $K_P = L_Q = \mathbb{Q}_2$. This implies the local square classes K_P^*/K_P^{*2} and L_Q^*/L_Q^{*2} are exactly same. This indicates that $\mathrm{Arf}(r_P) = \mathrm{Arf}(r_Q)$ and the corresponding Hilbert symbols are type I spaces since -1 is not a square in $\mathbb{Q}_2$. Also $\dim_{\mathbb{F}_2} K_P^*/K_P^{*2} = \dim_{\mathbb{F}_2} L_Q^*/L_Q^{*2} = 3$. If $p \equiv 5 \pmod 8$ or $p \equiv 3 \pmod 4$, then P and Q are inert or ramified primes. So $[K_P : \mathbb{Q}_2] = 2$ and $[L_Q : \mathbb{Q}_2] = 2$. The completions K_P and L_Q are the same field since $p \equiv q \pmod 8$. This implies that the local square classes are exactly same. So $\mathrm{Arf}(r_P) = \mathrm{Arf}(r_Q)$, $\mathrm{type}[(\ ,\ )_P] = \mathrm{type}[(\ ,\ )_Q]$ and $\dim_{\mathbb{F}_2} K_P^*/K_P^{*2} = \dim_{\mathbb{F}_2} L_Q^*/L_Q^{*2} = 4$. So we have a one to one correspondence

$$\{\text{dyadic place(s) in } K\} \xrightarrow{T_3} \{\text{dyadic place(s) in } L\}$$

satisfying $\mathrm{Arf}(r_P) = \mathrm{Arf}(r_{T_3P})$, $\mathrm{type}[(\ ,\ )_P] = \mathrm{type}[(\ ,\ )_{T_3P}]$, and $|K_P^*/K_P^{*2}| = |L_{T_3P}^*/L_{T_3P}^{*2}|$. Now we define a map

$$T : \Omega_K \longrightarrow \Omega_L,$$

where Ω_K and Ω_L are sets of places of K and L respectively, by

$$T(P) = \begin{cases} T_1(P) & \text{if } P \text{ is a non-dyadic split or inert place in } K \\ T_2(P) & \text{if } P \text{ is a non-dyadic ramified place in } K \\ T_3(P) & \text{if } P \text{ is a dyadic place in } K \\ \text{Archimedian place} & \text{if } P \text{ is an Archimedian place in } K \end{cases} \tag{3.34}$$

Then $\mathrm{Arf}(r_P) = \mathrm{Arf}(r_{TP})$, $\mathrm{type}[(r_P)] = \mathrm{type}[(r_{TP})]$, and $|K_P^*/K_P^{*2}| = |L_{TP}^*/L_{TP}^{*2}|$ for every place P in K. So K and L are Arf equivalent. □

3.4 Arf(r_P) for a Dyadic Split Prime P in Quadratic Fields

In the previous section we did not have to find local root numbers for dyadic places for quadratic number fields. Let $K = \mathbb{Q}(\sqrt{n})$ be a quadratic number field, where n is a square free integer and $n \equiv 1 \pmod 8$. Then $2O_K = PP'$ by Theorem 1.28, where P and P' are different prime ideals in O_K. Then $[K_P : \mathbb{Q}_2] = 1$. So $K_P = \mathbb{Q}_2$ and $\dim_{\mathbb{F}_2} K_P^*/K_P^{*2} = 2 + [K_P : \mathbb{Q}_2] = 3$. By Lemma 2.25 $\mathrm{Arf}(r_P)$ must be an eighth root of unity. In this section we find an eighth root of unity for $\mathrm{Arf}(r_P)$ by direct computations. Write

$$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = \{1, -1, 3, -3, 2, -2, 6, -6\}.$$

It is clear that $(a, b)_P = (a, b)_2$ for any $a, b \in \mathbb{Q}_2$ since $[K_P : \mathbb{Q}_2] = 1$. It is also clear that $r_P(1) = 1$. Note that the local absolute different D_{K_P} is $\mathbb{Z}_2 = (1)$ since

P is unramified.

(a) Define a map $\alpha_{-1} : \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \longrightarrow \{-1, 1\}$ by $\alpha_{-1}(x) = (-1, x)_2$. Then

$$\alpha_{-1}(1) = 1,$$

$$\alpha_{-1}(-1) = (-1,-1)_2 = (-1)^{(-1)\cdot(-1)} = -1,$$

$$\alpha_{-1}(3) = (-1,3)_2 = (-1)^{-1\cdot 1} = -1,$$

$$\alpha_{-1}(-3) = (-1,-3)_2 = (-1)^{(-1)\cdot(-2)} = 1,$$

$$\alpha_{-1}(2) = (-1,2)_2 = 1,$$

$$\alpha_{-1}(-2) = (-1,-2)_2 = (-1,-1)_2(-1,2)_2 = -1 \cdot 1 = -1,$$

$$\alpha_{-1}(6) = (-1,6)_2 = (-1,2)_2(-1,3)_2 = 1 \cdot (-1) = -1,$$

$$\alpha_{-1}(-6) = (-1,-6)_2 = (-1,2)_2(-1,-3)_2 = 1.$$

So we get $f_{\alpha_{-1}} = (2)^2$ since $\alpha_{-1}(1 + (2)^2) = 1$. This implies $\mathcal{N}f_{\alpha_{-1}} = 4$. So $f_{\alpha_{-1}} D_{K_P} = (4)$. By Theorem 2.13

$$\begin{aligned} r_P(-1) &= \frac{1}{\sqrt{4}} \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^2} \alpha_{-1}(4^{-1}x)\psi_{\mathbb{Q}_2}(4^{-1}x) \\ &= \frac{1}{2}(-1,4)_2 \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^2} \alpha_{-1}(x)\psi_{\mathbb{Q}_2}(\frac{x}{4}) \\ &= \frac{1}{2} \cdot 1 \cdot \{\alpha_{-1}(1) \cdot \psi_{\mathbb{Q}_2}(\frac{1}{4}) + \alpha_{-1}(3) \cdot \psi_{\mathbb{Q}_2}(\frac{3}{4})\} \\ &= \frac{1}{2}(e^{\frac{\pi i}{2}} - e^{\frac{3\pi i}{2}}) = i. \end{aligned}$$

(b) Define a map $\alpha_3 : \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \longrightarrow \{-1, 1\}$ by $\alpha_3(x) = (3, x)_2$. Then

$$\alpha_3(1) = 1, \ \alpha_3(-1) = (3,-1)_2 = (-1)^{1\cdot(-1)} = -1,$$

$$\alpha_3(3) = (3,3)_2 = (-1)^{1\cdot 1} = -1, \ \alpha_3(-3) = (3,-3)_2 = 1,$$

$$\alpha_3(2) = (3,2)_2 = -1, \ \alpha_3(-2) = (3,-2)_2 = 1,$$

$$\alpha_3(6) = (3,6)_2 = (3,3)_2(3,2)_2 = 1, \ \alpha_3(-6) = (3,-6)_2 = (3,-3)_2(3,2)_2 = -1.$$

So we get $f_{\alpha_3} = (2)^2$ since $\alpha_3(1 + (2)^2) = 1$. This implies $\mathcal{N}f_{\alpha_3} = 4$. So $f_{\alpha_3} D_{K_P} = (4)$. By Theorem 2.13

$$\begin{aligned} r_P(3) &= \frac{1}{\sqrt{4}} \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^2} \alpha_3(4^{-1}x)\psi_{\mathbb{Q}_2}(4^{-1}x) \\ &= \frac{1}{2} \cdot (3,4)_2 \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^2} \alpha_3(x)\psi_{\mathbb{Q}_2}(\frac{x}{4}) \\ &= \frac{1}{2} \cdot 1 \cdot \{\alpha_3(1) \cdot \psi_{\mathbb{Q}_2}(\frac{1}{4}) + \alpha_3(3) \cdot \psi_{\mathbb{Q}_2}(\frac{3}{4})\} \\ &= \frac{1}{2}(e^{\frac{\pi i}{2}} - e^{\frac{3\pi i}{2}}) = i. \end{aligned}$$

(c) Define a map $\alpha_{-3} : \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \longrightarrow \{-1, 1\}$ by $\alpha_{-3}(x) = (-3, x)_2$. Then

$$\alpha_{-3}(1) = 1, \ \alpha_{-3}(-1) = (5,7)_2 = 1,$$

$$\alpha_{-3}(3) = (5,3)_2 = 1, \ \alpha_{-3}(-3) = (5,5)_2 = 1,$$

$$\alpha_{-3}(2) = (5,2)_2 = -1, \ \alpha_{-3}(-2) = (5,14)_2 = (5,7)_2(5,2)_2 = -1,$$

$$\alpha_{-3}(6) = (5,6)_2 = (5,3)_2(5,2)_2 = -1, \ \alpha_{-3}(-6) = (5,10)_2 = (5,5)_2(5,2)_2 = -1.$$

So we get $f_{\alpha-3} = (1)$ since $\alpha_{-3}(1 + (2)) = 1$ and $1 + (2) = \mathbb{Z}_2^*$. This implies $\mathcal{N}f_{\alpha_{-3}} = 1$. So $f_{\alpha_{-3}} D_{K_P} = (1)$. By Theorem 2.13

$$\begin{aligned} r_P(-3) &= \frac{1}{\sqrt{1}} \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)} \alpha_{-3}(x)\psi_{\mathbb{Q}_2}(x) \\ &= \sum_{x=1} \alpha_{-3}(x)\psi_{\mathbb{Q}_2}(x) \\ &= \alpha_{-3}(1) \cdot \psi_{\mathbb{Q}_2}(1) = 1 \cdot e^{2\pi i} = 1. \end{aligned}$$

(d) Define a map $\alpha_2 : \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \longrightarrow \{-1, 1\}$ by $\alpha_2(x) = (2, x)_2$. Then

$$\alpha_2(1) = 1, \ \alpha_2(-1) = (2,-1)_2 = 1,$$

$$\alpha_2(3) = (2,3)_2 = -1, \ \alpha_2(-3) = (2,-3)_2 = -1,$$

$$\alpha_2(2) = (2,2)_2 = (2,-1)_2 = 1, \ \alpha_2(-2) = (2,-2)_2 = 1.$$

$$\alpha_2(6) = (2,6)_2 = (2,3)_2(2,2)_2 = -1, \ \alpha_2(-6) = (2,-6)_2 = (2,-2)_2(2,3)_2 = -1$$

So we get $f_{\alpha_2} = (2)^3$ since $\alpha_2(1 + (2)^3) = 1$. This implies $\mathcal{N}f_{\alpha_2} = 8$. So $f_{\alpha_2}D_{K_P} = (8)$. By Theorem 2.13

$$\begin{aligned} r_P(2) &= \frac{1}{\sqrt{8}} \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^3} \alpha_2(8^{-1}x)\psi_{\mathbb{Q}_2}(8^{-1}x) \\ &= \frac{1}{2\sqrt{2}} \ (2,8)_2 \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^3} \alpha_2(x)\psi_{\mathbb{Q}_2}(\frac{x}{8}) \\ &= \frac{1}{2\sqrt{2}} \cdot 1 \cdot \{\alpha_2(1) \cdot e^{\frac{\pi i}{4}} + \alpha_2(-1) \cdot e^{-\frac{\pi i}{4}} + \alpha_2(3) \cdot e^{\frac{3\pi i}{4}} + \alpha_2(-3) \cdot e^{-\frac{3\pi i}{4}}\} \\ &= \frac{1}{2\sqrt{2}} \ (e^{\frac{\pi i}{4}} + e^{-\frac{\pi i}{4}} - e^{\frac{3\pi i}{4}} - e^{-\frac{3\pi i}{4}}) = 1 \end{aligned}$$

(e) Define a map $\alpha_{-2} : \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \longrightarrow \{-1, 1\}$ by $\alpha_{-2}(x) = (-2, x)_2$. Then

$$\alpha_{-2}(1) = 1,$$

$$\alpha_{-2}(-1) = (-2,-1)_2 = (2,-1)_2(-1,-1)_2 = -1,$$

$$\alpha_{-2}(3) = (-2,3)_2 = 1,$$

$$\alpha_{-2}(-3) = (-2,-3)_2 = (2,-3)_2(-1,-3)_2 = -1,$$

$$\alpha_{-2}(2) = (-2,2)_2 = 1,$$

$$\alpha_{-2}(-2) = (-2,-2)_2 = (-2,2)_2(-2,-1)_2 = -1,$$

$$\alpha_{-2}(6) = (-2,6)_2 = (-2,2)_2(-2,3)_2 = 1,$$

$$\alpha_{-2}(-6) = (-2,-6)_2 = (-2,-2)_2(-2,3)_2 = -1.$$

So we get $f_{\alpha_{-2}} = (2)^3$ since $\alpha_{-2}(1 + (2)^3) = 1$. This implies $\mathcal{N}f_{\alpha_{-2}} = 8$. So $f_{\alpha_{-2}}D_{K_P} = (8)$. By Theorem 2.13

$$\begin{aligned} r_P(-2) &= \frac{1}{\sqrt{8}} \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^3} \alpha_{-2}(8^{-1}x)\psi_{\mathbb{Q}_2}(8^{-1}x) \\ &= \frac{1}{2\sqrt{2}} \ (-2,8)_2 \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^3} \alpha_{-2}(x)\psi_{\mathbb{Q}_2}(\frac{x}{8}) \\ &= \frac{1}{2\sqrt{2}} \{\alpha_{-2}(1) \cdot e^{\frac{\pi i}{4}} + \alpha_{-2}(-1) \cdot e^{-\frac{\pi i}{4}} + \alpha_{-2}(3) \cdot e^{\frac{3\pi i}{4}} + \alpha_{-2}(-3) \cdot e^{-\frac{3\pi i}{4}}\} \\ &= \frac{1}{2\sqrt{2}} \ (e^{\frac{\pi i}{4}} - e^{-\frac{\pi i}{4}} + e^{\frac{3\pi i}{4}} - e^{-\frac{3\pi i}{4}}) = i. \end{aligned}$$

(f) Define a map $\alpha_6 : \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \longrightarrow \{-1, 1\}$ by $\alpha_6(x) = (6, x)_2$. Then

$$\alpha_6(1) = 1,$$

$$\alpha_6(-1) = (6, -1)_2 = (2, -1)_2(3, -1)_2 = -1,$$

$$\alpha_6(3) = (6, 3)_2 = (2, 3)_2(3, 3)_2 = 1,$$

$$\alpha_6(-3) = (6, -3)_2 = (2, -3)_2(3, -3)_2 = -1,$$

$$\alpha_6(2) = (6, 2)_2 = (2, 2)_2(3, 2)_2 = -1,$$

$$\alpha_6(-2) = (6, -2)_2 = (6, -1)_2(6, 2)_2 = 1,$$

$$\alpha_6(6) = (6, 6)_2 = (3, 6)_2(2, 6)_2 = -1,$$

$$\alpha_6(-6) = (6, -6)_2 = 1,$$

So we get $f_{\alpha_6} = (2)^3$ since $\alpha_6(1 + (2)^3) = 1$. This implies $\mathcal{N} f_{\alpha_6} = 8$. So $f_{\alpha_6} D_{K_P} = (8)$. By Theorem 2.13

$$\begin{aligned} r_P(6) &= \frac{1}{\sqrt{8}} \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^3} \alpha_6(8^{-1}x)\psi_{\mathbb{Q}_2}(8^{-1}x) \\ &= \frac{1}{2\sqrt{2}} \; (6, 8)_2 \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^3} \alpha_6(x)\psi_{\mathbb{Q}_2}(\frac{x}{8}) \\ &= \frac{-1}{2\sqrt{2}} \{\alpha_6(1) \cdot e^{\frac{\pi i}{4}} + \alpha_6(-1) \cdot e^{-\frac{\pi i}{4}} + \alpha_6(3) \cdot e^{\frac{3\pi i}{4}} + \alpha_6(-3) \cdot e^{-\frac{3\pi i}{4}}\} \\ &= \frac{-1}{2\sqrt{2}} \; (e^{\frac{\pi i}{4}} - e^{-\frac{\pi i}{4}} + e^{\frac{3\pi i}{4}} - e^{-\frac{3\pi i}{4}}) = -i. \end{aligned}$$

(g) Define a map $\alpha_{-6} : \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \longrightarrow \{-1, 1\}$ by $\alpha_{-6}(x) = (-6, x)_2$. Then

$$\alpha_{-6}(1) = 1,$$

$$\alpha_{-6}(-1) = (-6, -1)_2 = (2, -1)_2(-3, -1)_2 = 1,$$

$$\alpha_{-6}(3) = (-6, 3)_2 = (-2, 3)_2(3, 3)_2 = -1,$$

$$\alpha_{-6}(-3) = (-6, -3)_2 = (2, -3)_2(-3, -3)_2 = -1,$$

$$\alpha_{-6}(2) = (-6, 2)_2 = (2, 2)_2(-3, 2)_2 = -1,$$

$$\alpha_{-6}(-2) = (-6, -2)_2 = (-6, -1)_2(-6, 2)_2 = -1,$$

$$\alpha_{-6}(6) = (-6,6)_2 = 1,$$

$$\alpha_{-6}(-6) = (-6,-6)_2 = (-6,2)_2(-6,3)_2 = 1.$$

So we get $f_{\alpha_{-6}} = (2)^3$ since $\alpha_{-6}(1+(2)^3) = 1$. This implies $\mathcal{N}f_{\alpha_{-6}} = 8$. So $f_{\alpha_{-6}} D_{K_P} = (8)$. By Theorem 2.13

$$\begin{aligned} r_P(-6) &= \frac{1}{\sqrt{8}} \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^3} \alpha_{-6}(8^{-1}x)\psi_{\mathbb{Q}_2}(8^{-1}x) \\ &= \frac{1}{2\sqrt{2}} \ (-6,8)_2 \sum_{x \in \mathbb{Z}_2^* \, mod^* \, (2)^3} \alpha_{-6}(x)\psi_{\mathbb{Q}_2}(\frac{x}{8}) \\ &= \frac{-1}{2\sqrt{2}} \cdot \{\alpha_{-6}(1) \cdot e^{\frac{\pi i}{4}} + \alpha_{-6}(-1) \cdot e^{-\frac{\pi i}{4}} + \alpha_{-6}(3) \cdot e^{\frac{3\pi i}{4}} + \alpha_{-6}(-3) \cdot e^{-\frac{3\pi i}{4}}\} \\ &= \frac{-1}{2\sqrt{2}} \ (e^{\frac{\pi i}{4}} + e^{-\frac{\pi i}{4}} - e^{\frac{3\pi i}{4}} - e^{-\frac{3\pi i}{4}}) = -1. \end{aligned}$$

So,

$$r_P(a) = \begin{cases} 1 & \text{if} \quad a = 1 \\ i & \text{if} \quad a = -1 \\ i & \text{if} \quad a = 3 \\ 1 & \text{if} \quad a = -3 \\ 1 & \text{if} \quad a = 2 \\ i & \text{if} \quad a = -2 \\ -i & \text{if} \quad a = 6 \\ -1 & \text{if} \quad a = -6. \end{cases} \tag{3.35}$$

Therefore

$$\text{Arf}(r_P) = \frac{1}{2\sqrt{2}} \sum_{x \in \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}} r_P(x) = \frac{1}{2\sqrt{2}}(2+2i) = \frac{1+i}{\sqrt{2}}.$$

The following table summarizes Theorem 2.13, previous Lemmas and Theorems in section 3.2 and section 3.3. Let $K = \mathbb{Q}(\sqrt{e \cdot n}\,)$, where $e = \pm 1$ and n is a square-free positive integer.

Summary of Results

place P	complex	real	non-dyadic		dyadic	
			split or inert	ramified	split	inert or ramified
$\dim_{\mathbb{F}_2} K_P^*/K_P^{*2}$	0	1	2	2	3	4
type$[(\ ,\ )_P]$	II	I	I or II	I or II	I	
Arf(r_P)	1	$\frac{1-i}{\sqrt{2}}$	1	± 1 or $\pm i$	$\frac{1+i}{\sqrt{2}}$	

Table 1

References

[1] C. Arf, *Untersuchungen über quadratische Formen in Körpern der Charakteristik 2*, J. Reine Angew. Math. 183 (1941), 148–167.

[2] G. Bachman, *Introduction to p-adic numbers and valuation theory*, Academic Press, 1964.

[3] J.P. Carpenter *Finiteness theorems for forms over global fields*, Math. Z. 209 (1992), no. 1, 153–166.

[4] J.W.S. Cassels, *Local fields*, Cambridge University Press, 1986.

[5] P.E. Conner and N. Yui, *The additive characters of the witt ring of an algebraic number field*, Canad. J. Of Math. 40, 1988.

[6] A. Czogała, *On reciprocity equivalence of quadratic number fields*, Acta Arith. 58 (1991), 27–46.

[7] A. Fröhlich and J. Queyrut, *On the functional equation of the Artin L-function for characters of real representations*, Inv. Math. 20 (1973) 125–138.

[8] K. Ireland and M. Rosen, *A Classical introduction to modern number theory*, Springer-Verlag, 1982.

[9] I. Kaplansky, *Linear algebra and geometry*, Dover Publications, 2003.

[10] Y. Kitaoka, *Arithmetic of quadratic forms*, Cambridge University Press, 1993.

[11] T.Y. Lam, *The algebraic theory of quadratic forms*, W.A. Benjamin, Inc., 1973.

[12] Serge Lang, *Algebraic number theory*, Springer, 1994.

[13] D.A. Marcus, *Number fields* Springer-Verlag, 1977.

[14] J. Martinet, *Character theory and Artin L-functions*, Academic Press, 1977, 1–87.

[15] O.T. O'Meara, *Introduction to quadratic forms*, Springer-Verlag, 1973.

[16] R. Perlis, *Arf equivalence I*, Number Theory in Progress, Vol I, 1997, 381–393.

[17] R. Perlis, K. Szymiczek, P.E. Conner, and R. Litherland, *Matching Witt rings with global fields*, Contemp. Math. 155, 1994, 365–387.

[18] A. Robert, *A course in p-adic analysis*, Springer-Verlag, 2000.

[19] W. Scharlau, *Quadratic and hermitian Forms*, Springer-Verlag, 1985.

[20] K. Szymiczek, *Bilinear algebra: An introduction to the algebraic theory of quadratic forms*, Gordon and Breach Science Publishers, 1997.

[21] J.T. Tate, *Local constants, Algebraic number fields (edited by A. Fröhlich)*, Academic Press, 1977, 89–131.

[22] E. Weiss, *Algebraic number theory*, Dover Publications, 1998.

Vita

Jeonghun Kim was born on December 9, 1970, in Mokpo, Korea. He finished his undergraduate studies in mathematics at Chonbuk National University in August 1997. In August 1999, he came to Louisiana State University to pursue graduate studies in mathematics. He earned a Master of Science degree from Louisiana State University in May 2001. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in August 2006.